December 30, 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. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations,[2] 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)).[3]

NERC is filing this Notice of Penalty with the Commission because Southwest Power Pool Regional Entity (SPP RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SPP RE's determination and findings of the violations of CIP Reliability Standards.

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of two hundred and thirty-five thousand dollars ($235,000), in addition to

[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 (2015). *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] 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.

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

other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Accordingly, NERC is filing the violations in this Full Notice of Penalty 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 by and between SPP RE and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

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

NERC Violation ID	Standard	Req	Discovery Method* Date	Penalty Amount
SPP2013013217	CIP-002-3	R3.1	SR	$235,000
SPP2013013218	CIP-003-3	R6	SR	
SPP2013013224	CIP-005-3a	R4.3, R4.5	SR	
SPP2013013225	CIP-006-3a	R2.2	SR	
SPP2013013226	CIP-007-3a	R1.1, R1.2, R1.3	SR	

NERC Violation ID	Standard	Req	Discovery Method* Date	Penalty Amount
SPP2013013227	CIP-007-3a	R2.1	SR	$235,000
SPP2013013231	CIP-007-3a	R6.2, R6.4	SR	
SPP2014013561	CIP-005-3a	R3.2	SC	
SPP2014013565	CIP-007-3a	R3.1, R3.2	SC	
SPP2014013566	CIP-007-3a	R8.4	SC	

SPP2013013217 CIP-002-3- OVERVIEW

SPP RE determined that URE did not maintain a complete list of Critical Cyber Assets (CCAs). URE installed human machine interface client software, which is used to access URE's supervisory control and data acquisition/energy management system (SCADA/EMS) on devices, including workstations, desktops, and laptops, all of which were outside of URE's Electronic Security Perimeter (ESP). URE failed to include these devices on its CCA list as required by CIP-002-3 R3.1.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). This violation presented the risk that the SCADA/EMS could be compromised because the human machine interface client software could allow a direct connection to the production EMS from the devices on which the client software was installed, and these devices were neither identified nor protected as CCAs. The software deployments were installed on devices outside the ESP, including laptops used primarily for after-hours on-call support; virtual workstations used by distribution operators; and desktops in the organization. The software was installed on six desktops inside the ESP that were listed as CCAs, but not afforded CIP protections. The workstations used by the distribution operators were protected by the ESP firewall. Of the 120 users with access via the software, only 22 (18%) had administrative rights for the SCADA/EMS. The 22 users received access based on a business need, completed NERC training (CIP and Operations and Planning), and had current personnel risk assessments (PRA). These users were comprised of EMS and transmission

planning staff. URE maintained strong authentication access controls for the users, such as requiring an appropriate individual username and password, token authorization, and firewall authorization. The remaining users were granted read-only access rights to the EMS.

SPP RE determined the duration of the violation to be from the day after the completion of the previous audit, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010511 to address the referenced violations. URE's Mitigation Plan required URE to:

1. conduct an infrastructure and architecture review of its full environment;
2. appropriately classify devices (newly identified and existing) based on its methodology, and modify its master CIP device list;
3. commission newly identified assets according to URE's processes;
4. implement a commissioning process for all existing devices on its master CIP device list;
5. train and provide communications materials to affected personnel on URE's inventory and commissioning processes; and
6. add a quality review step within URE's commissioning process for compliance validation prior to putting an asset in service.

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

SPP2013013218 CIP-003-3- OVERVIEW

SPP RE determined that URE did not adhere to its change control and configuration management process. Specifically, URE personnel made changes to an Electronic Access Control and Monitoring System (EACMS) in the production environment, rather than in the test environment. Additionally, an approved change management request was not acquired before patches were installed on four EACMS and a Physical Access Control System (PACS), and group policy settings were made in URE's production environment.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-003 R6 has the potential to compromise the reliable operation of the BPS by exposing CCAs to potential vulnerabilities resulting from application of undocumented change control or configuration management activities. Notwithstanding, URE did have protective measures in places that reduced the risk. For example, all of the affected devices resided within URE's

ESP; URE was logging and monitoring access to these devices for potential security events; and URE's CCAs were protected by firewalls specifically configured to allow only authorized traffic to enter the network, thereby preventing unsolicited traffic from passing into the ESP. URE also utilized a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to CCAs was limited to those individuals with authorized physical and/or electronic access rights, all of whom had completed CIP training and possessed current personnel risk assessments.

SPP RE determined the duration of the violation to be from the completion date of URE's mitigation plan for previous violations of the same standard and requirement, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT011015 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise its change control and management process to include additional steps, i.e., a sign-off checklist, to ensure adherence to the process;
2. implement preventive and detective controls to identify or disable the ability to implement changes to CCAs in other than the test environment; and
3. provide training to all affected staff.

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

SPP2013013224 CIP-005-3a - OVERVIEW

SPP RE determined that URE's Cyber Vulnerability Assessments (CVAs) for two calendar years did not include a visual inspection of physical devices to verify that all electronic access points to the ESP were identified (R4.3). Additionally, the CVA results did not include action plans to remediate or mitigate potential vulnerabilities identified by the CVAs (R4.5).

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. When potential cyber security vulnerabilities are left unresolved or unmitigated, they create the opportunity to exploit those vulnerabilities thereby exposing devices to potential cyber attack. Failing to identify all access points to the ESP also increases the risk of cyber attack because such access points may not be afforded adequate security measures. Nevertheless, the CVAs addressed requirements R4.1, R4.2, and R4.4. For example, URE's maintained a document identifying the vulnerability assessment process (R4.1); conducted reviews to verify that only ports and services

required for operations at access points to the ESP were enabled (R4.2); and reviewed controls for default accounts, passwords, and network management community strings (R4.4). URE was logging and monitoring identified access points to its ESP. Additionally, URE maintained firewalls that were configured to allow only electronic traffic using specific protocols to enter the network, which prevented unauthorized access to the ESP. Network traffic, at URE's ESP access points, was analyzed for known and suspected malicious activity using a network intrusion detection system. Access to all Cyber Assets inside the ESP was limited to only those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the publication date of the CVA report for the first calendar year, through when the URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010972 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise its CVA process to:
    a. require visual inspections of physical devices located within the ESP;
    b. require action plans to remediate or mitigate potential vulnerabilities identified in the CVAs;
2. provide training to all affected staff; and
3. conduct a CVA that included the above revisions to the CVA process.

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

SPP2013013225 CIP-006-3a- OVERVIEW

SPP RE determined that URE did not afford all of the protective measures specified in CIP-003-3 R6 and CIP-007-3 R1, R3, R5.3.3, and R6 to some PACS devices.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. By not affording CIP protections to the PACS, the risk existed that the Physical Security Perimeter (PSP) could be compromised. SPP RE determined that no breach of URE's PSP, CCAs, or data resulted from a lack of change control or configuration management of the PACS. URE's Cyber Assets were protected by firewalls configured to allow only traffic using specific protocols to enter the network, which prevented unsolicited traffic from passing into the ESP. URE also used system logging to analyze network traffic at access points to the ESP for known and suspected

malicious activity. Access to CCAs was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE 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 designated SPPMIT010973 to address the referenced violations. URE's Mitigation Plan required URE to:

1. upgrade its servers to provide sustainable support;
2. conduct infrastructure and architecture review of the full system environment;
3. assess all devices using updated classification methodology and appropriately record those on the master CIP device list;
4. commission newly identified assets according to established processes;
5. implement a commissioning process for all CIP-related cyber assets identified or existing on master CIP device list;
6. train applicable personnel and distribute communications materials on its inventory and commissioning processes; and
7. institute a quality review step within its commissioning process for compliance validation prior to assets being placed in service.

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

SPP2013013226 CIP-007-3a - OVERVIEW

SPP RE determined that URE did not ensure that significant changes to Cyber Assets within the ESP did not adversely affect existing cyber security controls.

URE did not test multiple significant changes to Cyber Assets within the ESP prior to implementing the changes in the production environment. Additionally, an information technology technician scheduled patching for Cyber Assets in the test environment and mistakenly included a production PACS device in the automated system used for downloading patches. Accordingly, URE failed to ensure that significant changes to existing Cyber Assets within the ESP did not adversely affect existing cyber security controls.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-007 R1 provides the opportunity for new Cyber Assets within the ESP and significant changes to existing Cyber Assets within the ESP to adversely affect existing cyber security controls. Notwithstanding, URE had implemented security controls test procedures and tested most changes in accordance with such procedures. The identified Cyber Assets were located within a PSP. In addition, all network traffic that was within the ESP was logged and monitored by URE's system log server, which was configured to send alerts to IT personnel had any unusual traffic been suspected. URE's CCAs were protected by a firewall configured to allow only traffic using specific protocols to enter the network, which prevented unsolicited traffic from passing into the ESP. The URE also used a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to CCAs was limited to only those individuals with authorized physical and/or electronic access rights. The URE discovered the violation as part of its Internal Compliance Program review processes.

SPP RE determined the duration of the violation to be from the completion date of URE's mitigation plan for previous violations of the same standard and requirement, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010971 to address the referenced violations. URE's Mitigation Plan required URE to:

1. enhance its existing cyber security controls test process and institute technical or procedural controls to ensure that testing minimizes the impact to production systems;
2. institute quality assurance steps in its current change management process, including cyber security controls test validation;
3. implement a sign-off check list for the quality assurance steps in the change management process;
4. institute preventive/detective controls to identify or disable the possibility to confuse environments for changes or testing; and
5. deliver training and distribute awareness communications (cyber security controls test and current change management process changes) to applicable staff.

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

SPP2013013227 CIP-007-3a - OVERVIEW

SPP RE determined that URE did not include some CCAs in its ports and services control procedure. As a result, URE was unable to ensure that only those ports and services required for normal and emergency operations were enabled.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-007-3a R2.1 has the potential to allow the infiltration of unauthorized network traffic into the ESP through ports and services that are not necessary for normal or emergency operations. Although URE had not identified all of it CCAs, it had implemented a process to regularly review ports and services of CCAs. The devices in question were located within an ESP and PSP. In addition, all network traffic within its ESP was logged and monitored by URE's system log server, which was configured to send alerts to IT personnel when any unusual traffic is identified. URE's CCAs were protected by firewalls configured to allow only traffic using specific protocols to enter the network, which prevents unsolicited traffic from passing into the ESP. URE also used a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to CCAs was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the date after the completion of the previous audit, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010478 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop a process to establish and maintain a baseline of ports and services and workflow to ensure only those ports and services that are required for normal and emergency operation are enabled;
2. institute preventive or detective controls (i.e., exception reporting, etc.) for ports and services to identify additions or changes;
3. institute preventive/detective controls to identify or disable the possibility to confuse environments for changes or testing; and
4. deliver ports and services training to applicable staff.

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

SPP2013013231 CIP-007-3a - OVERVIEW

SPP RE determined that URE did not correctly format four automated alerts, which prevented the issuance of automated alerts for detected cyber security incidents. However, during further discussions with URE, SPP RE determined that URE had an additional instance of noncompliance with CIP-007-3a R6.2 and an instance of noncompliance with R6.4.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-007 R6 has the potential to allow the compromise of CCAs and other system cyber security events to occur without URE's knowledge. Where automated alerting was not generated because the logs were not sent to the centralized logging server, the logs were retained at the devices. The period that logs were not captured was limited to maintenance outages. URE manually monitored the centralized logging server on a daily basis during business hours for any logging failures (missing logs or invalid formats).

Regarding this instance of noncompliance, URE maintained firewalls that were configured to allow only electronic traffic using specific protocols to enter the network, which prevented unsolicited traffic from passing into the ESP. URE also utilized a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to Cyber Assets inside the ESP was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the date after the completion of the previous audit, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010477 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop and implement a new process to identify logging and alerting failures;
2. implement an alternative technology to replace the centralized logging server;
3. implement a commissioning process for CIP-related cyber assets to include validation of alerting, capture of electronic logs, and retention of such logs; and
4. provide training to all affected staff.

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

SPP2014013561 CIP-005-3a - OVERVIEW

SPP RE determined that URE did not monitor all access points to the ESP for attempted or actual unauthorized access, twenty-four hours a day, seven days a week.

URE's satellite clocks were electronic access points (EAPs) located inside URE's ESP. The clocks were used to provide global position system data to establish time values, and were serially connected to URE's EMS data acquisition servers, which were CCAs located in URE's ESP. It was technically infeasible for the clocks to alert for attempts at or actual unauthorized access to the ESP; however, URE failed to file a Technical Feasibility Exception (TFE) with SPP RE.

URE's modem sharing devices were EAPs located inside URE's ESP and communicated with its field Remote Terminal Units (RTUs). It was technically infeasible for these modem sharing devices to alert for attempts at or actual unauthorized access to the ESP; however, URE failed to file a TFE with SPP RE.

During an audit, SPP RE discovered two EACMs/EAP devices and two CCA devices that were continually logging access to the ESP, which were sent to the centralized logging server. However, it was technically infeasible for the server to generate automated alerts for attempts at or actual unauthorized access to the ESP, and URE failed to file a TFE with SPP RE.

As to the above instance of noncompliance, URE was not reviewing or otherwise assessing access logs for attempts at or actual unauthorized access at least every ninety calendar days.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-005-3a R3 provides the opportunity for access attempts or unauthorized access to the ESP to occur without URE's knowledge. Notwithstanding URE's failure to implement the mitigating measures associated with TFEs, URE had implemented a documented process for monitoring and logging access at access points to the ESP. URE's firewalls were configured to allow only electronic traffic using specific protocols to enter the network, which prevents unsolicited traffic from passing into the ESP. URE also used a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to all Cyber Assets within the ESP was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the date after the completion of the previous audit, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT011019 to address the referenced violations. URE's Mitigation Plan required URE to:

1. implement an enhanced commissioning process including TFE identification on CIP-related Cyber Assets;
2. implement tools for monitoring, alerting, and retaining logs for applicable CIP-related Cyber Assets;
3. develop a process to identify and remediate gaps in monitoring or alerting; and
4. deliver training to applicable staff.

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

SPP2014013565 CIP-007-3a - OVERVIEW

SPP RE determined that URE's centralized logging server was utilized for electronic access control and monitoring of Cyber Assets located within URE's ESP. Available security patches for the centralized logging server were not evaluated, tested, or installed (R3.1), and no compensating measures were applied to mitigate risk exposure (R3.2).

During an audit, SPP RE discovered additional instances of noncompliance with CIP-007-3a R3.1 and R3.2. A security patch for six network switches was not installed (R3.1), and no compensating measures were applied to mitigate risk exposure (R3.2).

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-007-3a R3 provides the opportunity for infiltration of unauthorized network traffic into the ESP when security patches and upgrades are not installed on Cyber Assets within the ESP. All network traffic within URE's ESP was logged and monitored by URE's system log server, which is configured to send alerts to IT personnel when any unusual traffic is identified. URE's CCAs were protected by firewalls configured to allow only traffic using specific protocols to enter the network, which prevents unsolicited traffic from passing into the ESP. URE also used a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to CCAs was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the completion date of URE's mitigation plan for previous violations of the same standard and requirement, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT011021 to address the referenced violations. URE's Mitigation Plan required URE to:

1. execute its commissioning process, including TFE identification, for all CIP-related cyber assets identified or existing on the master CIP device list;
2. enhance its patch management processes for consistency in tracking and monitoring applicable patches and compensating measures for CIP related Cyber Assets;
3. integrate patch management processes with change and configuration management processes; and
4. train applicable personnel and provide communication materials on the inventory and commissioning process.

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

SPP2014013566 CIP-007-3a - OVERVIEW

SPP RE determined that URE did not include action plans to remediate or mitigate potential vulnerabilities identified in the CVAs for two calendar years.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Failure to mitigate vulnerabilities identified in the CVA assessment and track the implementation of corrective action plans has the potential to allow vulnerabilities to continue unmitigated. Notwithstanding, URE conducted CVAs in those calendar years that addressed the remainder of the required information prescribed in R8. URE was logging and monitoring Cyber Assets within its ESP. URE maintained firewalls that were configured to allow only electronic traffic using specific protocols to enter the network, which prevented unsolicited traffic from passing into the ESP. URE also utilized a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to Cyber Assets inside the ESP was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the publication date of the first CVA Report, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010929 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise its CVA process to require action plans to remediate or mitigate potential vulnerabilities identified in the CVAs;
2. provide training to all affected staff; and
3. conduct a CVA inclusive of the above revisions to the CVA process.

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

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SPP RE has assessed a penalty of two hundred and thirty-five thousand dollars ($235,000) for the referenced violations. In reaching this determination, SPP RE considered the following factors:

1. SPP RE considered URE's compliance history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violation which SPP RE considered as a neutral factor in penalty determination;
3. URE self-reported three violations, but did not receive mitigating credit for seven other violations because they were submitted approximately four months prior to a Compliance Audit, which was after receiving notice of the upcoming audit;
4. URE was cooperative throughout the compliance enforcement process;
5. URE did not evidence any attempt to conceal a violation nor the intent to do so;
6. all of the violations posed a moderate but not a serious or substantial risk to the reliability of the BPS; and
7. SPP RE found there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SPP RE determined that, in this instance, the penalty amount of two hundred and thirty-five thousand dollars ($235,000) 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 December 16, 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.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred and thirty-five thousand dollars ($235,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

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

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

cc: Unidentified Registered Entity
Southwest Power Pool Regional Entity

Attachments