**PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION**

December 30, 2014

**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# NCRXXXXXX, 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 Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE agrees and stipulates to the violations, and has agreed to the assessed penalty of one hundred twenty thousand dollars ($120,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under 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.

terms and conditions of the 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. 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 Standard | Req. | VRF/ VSL* | Total Penalty |
|---|---|---|---|---|
| WECC2013012030 | CIP-002-1 | R3 | Lower/ Severe | $120,000 |
| WECC2013012032 | CIP-004-1 | R2; R2.2 | Medium/ Severe | |
| WECC2013012685 | CIP-004-1 | R4; R4.1 | Lower/ High | |

| NERC Violation ID | Reliability Standard | Req. | VRF/ VSL* | Total Penalty |
|---|---|---|---|---|
| WECC2013012326 | CIP-005-1 | R1; R1.5 | Medium/ Severe | $120,000 |
| WECC2013012935 | CIP-005-1 | R2; R2.1 | Medium/Severe | |
| WECC2013012937 | CIP-005-3a | R4 | Medium/Severe | |
| WECC2013012327 | CIP-006-1 | R1; R1.8 | Medium/ Severe | |
| WECC2013012946 | CIP-006-3c | R8 | Medium/Severe | |
| WECC2013012939 | CIP-007-1 | R5; R5.2 | Lower/ Severe | |
| WECC2013012940 | CIP-007-1 | R6; R6.1 | Medium/ Severe | |
| WECC2013012938 | CIP-007-3a | R8; R8.4 | Medium/ Severe | |
| WECC2013012033 | CIP-009-1 | R1 | Medium/ Severe | |
| WECC2013012034 | CIP-009-2 | R4 | Lower/ Severe | |

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

CIP-002-1 R3 (WECC2013012030)

URE submitted a Self-Certification stating that it was in violation of CIP-002 R3. URE failed to include three Cyber Assets on its list of Critical Cyber Assets (CCAs). The purpose of the devices is to convert remote terminal unit (RTU) data from transmission control protocol/internet protocol into serial communications data and back. The root cause of the violation was determined to be human error, related to URE's initial assessment that the devices did not have routable protocol.

WECC determined that URE had a violation of CIP-002-1 R3 for failing to include three Cyber Assets on its list of associated CCAs essential to the operation of the Critical Asset.

WECC 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.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). All of the devices were located inside a Physical Security Perimeter (PSP) and Electronic Security Perimeter (ESP). Physical and logical access was limited to only authorized URE staff with the appropriate authorizations to access each device.

URE's Mitigation Plan to address this violation was submitted to WECC. URE's Mitigation Plan required URE to add the three Cyber Assets to its Cyber Asset hardware list and clarify the specific asset types in the list.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-004-1 R2; R2.2 (WECC2013012032)

URE submitted a Self-Certification to WECC stating that it was in violation of CIP-004 R2. URE failed to review its cybersecurity training program for one year. In addition, URE's program did not include the items required by CIP-004-1 R2.2.1-R2.2.4. Specifically, URE's training material did not specifically train individuals on: (i) the proper use of CCAs; (ii) physical and electronic access controls to CCAs; (iii) the proper handling of CCA information; and (iv) action plans and procedures to recover or re-establish CCAs and access thereto following a Cyber Security Incident. While WECC determined that this

information was covered in URE's separate awareness training, it was not included as part of URE's cybersecurity training program as required by the Standard.

WECC determined that URE had a violation of CIP-004-1 R2 for failing to review its cybersecurity training program annually and for failing to include all of the required topics.

WECC 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.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE reviewed its training program in the year before and the year after the violation year. URE conducted training for all personnel who had authorized unescorted logical or physical access. The cybersecurity training program familiarized personnel with the language and procedures of the CIP standards. While the training program did not meet all of the requirements of CIP-004 R2, it did include training on the CIP-002 through CIP-009 standards and URE's policies and procedures. Additionally, although URE's cybersecurity training did not specifically cover all required areas, URE's additional cybersecurity awareness training, which was provided upon initial implementation of the CIP program, did cover these areas. Further, URE conducted quarterly awareness activities to reinforce security practices.

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

URE's Mitigation Plan required URE to:

1. update the training program document to reflect more accurately the training being conducted;
2. review and incorporate the cybersecurity training presentation; and
3. conduct training for all personnel with unescorted logical or physical access using a revised and formalized cybersecurity awareness training presentation which includes all the required components of the Standard.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-004-1 R4; R4.1 (WECC2013012685)

URE submitted a Self-Report stating that it was in violation of CIP-004-1 R4. WECC conducted a Compliance Audit of URE (Compliance Audit). During the Compliance Audit, WECC staff reviewed the scope of URE's Self-Report.

WECC determined that URE failed to maintain its list of personnel with authorized cyber access to CCAs in two instances. In the first instance, URE updated its list 21 days prior to granting logical access to an employee. URE updated its list within seven days of access being authorized, not access being granted. In the second instance involving a different employee, URE updated its list one month after logical access was granted.

WECC determined that URE had a violation of CIP-004-1 R4 for failing to maintain its list of personnel with authorized Cyber Assets to CCAs and update the list within seven calendar days of any change.

WECC determined the duration of the violation for the first instance to be from the date URE changed its access list prior to access being granted through the date URE granted access to that employee. WECC determined the duration of the violation for the second instance to be from the eighth day after URE granted access to the employee through the date URE updated its access list to reflect this change.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Both individuals who were granted access received CIP training and had completed Personnel Risk Assessments. The issue was limited to the failure to update the list in a timely manner; no access to CCAs was granted to unauthorized personnel. Both individuals had "need to know" local access to CCAs.

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

URE's Mitigation Plan required URE to:

1. modify the steps it uses to grant or revoke access to include additional tracking and controls; and
2. confirm that access lists were current.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-005-1 R1; R1.5 (WECC2013012326)

WECC contacted URE to discuss URE's Self-Certifications of CIP-009 R1 and CIP-009 R4 (WECC2013012033 and WECC2013012034, respectively). During this discussion, URE stated that the scope of these violations included four devices used in the electronic access control and monitoring (EACM) of two ESPs. The EACM devices consisted of modems, servers, and firewalls.

WECC determined that URE had a violation of CIP-005-1 R1 for failing to afford all of the protections required by CIP-005-1 R1.5 (specifically, CIP-003 R4, CIP-009 R1, and CIP-009 R4) to EACM devices used to monitor two ESPs.

WECC 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.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE maintained the EACM devices within a PSP. Access to the PSP was restricted, actively monitored, and logged. Only authorized individuals were permitted to access the PSP. URE had written maintenance agreements with vendors to contact URE within eight hours and restore the devices if URE encountered an issue. URE had backup and restore procedures in place for Windows devices, and it was recording tape backups regularly.

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

URE's Mitigation Plan required URE to:

1. revise its information protection plan;
2. classify all documents as required by the plan that were not previously marked as information associated with CCAs; and
3. update its recovery plan to include EACM devices, including backup media.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-005-1 R2; R2.1 (WECC2013012935)

During the Compliance Audit, WECC discovered that URE failed to provide required access point security controls for two access points to the ESPs in violation of CIP-005 R2. Two servers did not

provide the ability to specify explicit access permission for all communication at these access points. Further, one of the access points did not provide strong network separation between two ESPs and the physical security network.

WECC determined that URE had a violation of CIP-005-1 R2 for failing to ensure that the two access points to the ESP used an access control model that denied access by default, such that explicit access permissions must be specified.

WECC determined the duration of the violation to be from when one of the two access points was installed through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE locked down the devices to disable routing across its interfaces. The devices had antivirus and other CIP-007 protections, such as patching and logging. The devices were performing real-time logging and monitoring of all traffic. The devices were protected by firewalls with explicit rules for all traffic. The devices were within a defined PSP. There was no interactive access into any ESP or across the access point boundary, except emergency vendor modem access with defined manual procedures to enable this access. Further, the access points at issue were used only to collect logs and generate alerts from ESP devices and physical access control system (PACS) devices.

URE's Mitigation Plan to address this violation was submitted to WECC stating it had been completed.

URE's Mitigation Plan required URE to:

1. move the two devices out of the ESP and into a demilitarized zone with explicit access lists to allow proper network traffic flow for collection of security events from ESP CCA devices; and
2. reclassify the devices as monitoring devices of the ESP.

CIP-005-3a R4 (WECC2013012937)

During the Compliance Audit, WECC discovered that URE failed to conduct an annual Cyber Vulnerability Assessment (CVA) for one access point in violation of CIP-005-3a R4. URE failed to include the configuration information for a dial-up accessible modem to the third party conducting the annual CVAs for URE. WECC also discovered that URE failed to document the execution status of its action plan to remediate or mitigate vulnerabilities identified in the CVAs for two calendar years for all four of its access points.

WECC determined that URE had a violation of CIP-005-3a R4 for failing to perform a CVA for one access point and for failing to document the execution status of the action plan to remediate or mitigate vulnerabilities in the CVA for four access points.

WECC determined the duration of the violation to be from the last date in the first calendar year it could have complied with the annual CVA requirement through the last date in the second calendar year it could have complied with the annual CVA requirement.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented a defense-in-depth architecture designed to prevent malicious cyber attacks. Specifically, URE used various physical and logical cybersecurity controls, physical security mechanisms (special locks and closed circuit television), additional firewalls, vulnerability scanning tools, and internal cybersecurity controls.

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

URE's Mitigation Plan required URE to:

1. remove the modem from service and the CIP asset inventory; and
2. conduct the annual CVA to get a new baseline of action plans for the devices, and create additional tracking mechanisms to ensure the action plans and execution status are updated.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-006-1 R1; R1.8 (WECC2013012327)

WECC contacted URE to discuss URE's Self-Certifications of CIP-009 R1 and CIP-009 R4 (WECC2013012033 and WECC2013012034, respectively). During the interview, URE stated that the scope of these violations included 10 devices used in the physical access control and monitoring of two PSPs. The devices consisted of workstations, servers, controllers, and switches.

WECC determined that URE had a violation of CIP-006-1 R1 for failing to provide several of the protections specified in R1.8 (specifically, CIP-003 R4, CIP-009 R1, and CIP-009 R4) to Cyber Assets used in the access control and monitoring of the PSPs.

WECC 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.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE maintained the devices within an ESP. Access to the ESP was restricted, actively monitored, and logged. Many of the devices were redundant; failure of these devices would not affect URE's network infrastructure. URE had written maintenance agreements with vendors to contact URE within eight hours and restore the devices if URE encountered an issue. URE had backup and restore procedures in place for Windows devices and was recording tape backups regularly.

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

URE's Mitigation Plan required URE to:

1. revise its information physical access protection plan and mark all documents as required by the plan that were not previously marked; and
2. update its recovery plan to include CIP-006 assets, including protective measures from unauthorized physical access.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-006-3c R8 (WECC2013012946)

During the Compliance Audit, WECC discovered that URE failed to implement a maintenance and testing program that ensured all of the physical security systems under Requirements R4, R5, and R6 functioned properly, in violation of CIP-006-3c R8. Specifically, URE did not conduct the testing of specified controls at each PSP access point during maintenance and testing activities. The testing included some maintenance activities, such as cleaning camera lenses and updating software, but did not include testing of door alarms, glass break sensors, or logging of alarms in the PACS system.

WECC determined that URE had a violation of CIP-006-3c R8 for failing to implement a maintenance and testing program to ensure that all physical security systems under R4, R5, and R6 functioned properly.

WECC determined the duration of the violation to be from one month past the prior audit interval through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had multiple layers of security. The PSPs were staffed at all times and/or protected by fencing. URE's contractor was performing preventative maintenance activities on a semi-

annual basis. Further, URE provided evidence showing that, as of a certain date, the physical security systems for a PSP area were tested to meet its installation requirements.

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

URE's Mitigation Plan required URE to:

1. update its maintenance and testing procedure;
2. develop a checklist and sign-off sheet; and
3. schedule maintenance with vendor to conduct maintenance as prescribed in new plan.

CIP-007-1 R5; R5.2 (WECC2013012939)

During the Compliance Audit, WECC discovered that URE was in violation of CIP-007 R5. URE failed to remove, disable, or rename the built-in Windows administrator account on one PACS device as required by R5.2.1.

WECC determined that URE had a violation of CIP-007-1 R5 for failing to implement a policy to remove, disable, or rename a built-in administrator account on a PACS device.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE deactivated the administrator account during the Compliance Audit.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This was an isolated event, and the account did not have a default password assigned. URE had changed the password at least once, but not annually, after enabling the account. Further, URE implemented a defense-in-depth architecture of physical and logical cybersecurity controls, including physical security mechanisms, special locks, closed circuit television, and logical perimeter and internal cybersecurity controls, including firewalls, vulnerability scanning tools, and a security events management system.

URE's Mitigation Plan to address this violation was submitted to WECC. URE's Mitigation Plan required URE to disable the account.

URE certified that the above Mitigation Plan requirement was completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-007-1 R6 (WECC2013012940)

During the Compliance Audit, WECC discovered that URE had a violation of CIP-007 R6. URE failed to provide sufficient evidence of security event monitoring for one CCA, a video display board.

WECC determined that URE had a violation of CIP-007-1 R6 for failing to implement and document the organizational processes and technical and procedural mechanisms for monitoring system events related to cybersecurity for one CCA within the ESP.

WECC 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.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The violation was isolated and affected only one device. URE implemented a defense-in-depth architecture of physical and logical cybersecurity controls, including physical security mechanisms, special locks, closed circuit television, and logical perimeter and internal cybersecurity controls, including firewalls, vulnerability scanning tools, and a security events management system.

URE's Mitigation Plan to address this violation was submitted to WECC stating it had been completed.

URE's Mitigation Plan required URE to:

1. monitor the video board device; and
2. provide evidence of logging for 90 days.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-007-3a R8; R8.4 (WECC2013012938)

During the Compliance Audit, WECC discovered that URE had a violation of CIP-007-3a R8. URE failed to document the execution status columns of the action plans to remediate or mitigate vulnerabilities identified during the CVAs of all Cyber Assets within the ESP for two calendar years due to staffing shortfalls.

WECC determined that URE had a violation of CIP-007-3a R8 for failing to document the execution status of the action plans for two CVAs.

WECC determined the duration of the violation to be from the last date in the first calendar year URE could have complied with the annual CVA requirement through the last date in the second calendar year URE could have complied with the annual CVA requirement.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented a defense-in-depth architecture of physical and logical cybersecurity controls, including physical security mechanisms with guards, special locks, closed circuit television, and logical perimeter and internal cybersecurity controls, including firewalls, vulnerability scanning tools, and intrusion detection systems.

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

URE's Mitigation Plan required URE to:

1. conduct an annual CVA to get a new baseline of action plans for the devices; and
2. create additional tracking mechanisms to ensure the action plans and execution status are updated.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-009-1 R1 (WECC2013012033)

URE submitted a Self-Certification stating it was in violation of CIP-009 R1. URE failed to create a recovery plan for CCAs that specified the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan. In addition, WECC determined that URE's recovery plan did not address any networking CCAs or non-critical Cyber Assets.

WECC determined that URE had a violation of CIP-009-1 R1 for failing to create a recovery plan for all CCAs and for failing to ensure that the plan specified the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan.

WECC 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.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had vendor service agreements in place to aid in the recovery of CCAs. Many of the non-Windows devices were redundant, such that URE's business would not be impacted

by a single failure. Further, URE's information technology personnel responsible for recovery had practical knowledge of the devices and therefore had the experience to recover CCAs in the event of a Cyber Security Incident.

URE's Mitigation Plan to address this violation was submitted to WECC. URE's Mitigation Plan required URE to update its recovery plan.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-009-2 R4 (WECC2013012034)

URE submitted a Self-Certification stating that it was in violation of CIP-009 R4. URE failed to include processes and procedures for the backup and storage of information required to successfully restore network switches, firewalls, terminal servers, and control panels. Specifically, URE's backup and restore procedures did not contain sufficient detail and listed as resources only the vendor recovery documentation (however, the procedures did not provide the locations of the vendor documentation).

WECC determined that URE had a violation of CIP-009-2 R4 for failing to ensure that the recovery plan included processes and procedures for the backup and storage of information required to successfully restore CCAs.

WECC determined the duration of the violation to be from the day after WECC previously notified URE that it was compliant with the Standard through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE maintained the devices within an ESP, access to which was restricted, actively monitored, and logged. Many of the devices were redundant; therefore, failure of these network devices would not affect URE's network infrastructure. URE had written maintenance agreements with vendors to contact URE within eight hours and restore the devices if URE encountered an issue. Further, URE had backup and restore procedures in place for Windows devices and was recording tape backups regularly.

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

URE's Mitigation Plan required URE to update its process document to include detailed steps describing how URE conducts its backup procedures.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred twenty thousand dollars ($120,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's prior violations as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violation which WECC considered a mitigating factor;
3. URE was cooperative throughout the compliance enforcement process;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. URE took voluntary corrective action to remediate this violation, which WECC considered a mitigating factor;
6. the violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; 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, WECC determined that, in this instance, the penalty amount of one hundred twenty thousand dollars ($120,000) 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 18, 2014 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 WECC as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred twenty thousand dollars ($120,000) 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.

**Attachments to be Included as Part of this Notice of Penalty**

REDACTED FROM THIS PUBLIC VERSION

[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<br>President and Chief Executive Officer<br>North American Electric Reliability Corporation<br>3353 Peachtree Road NE<br>Suite 600, North Tower<br>Atlanta, GA 30326<br>(404) 446-2560<br><br>Charles A. Berardesco*<br>Senior Vice President and General Counsel<br>North American Electric Reliability Corporation<br>1325 G Street N.W., Suite 600<br>Washington, DC 20005<br>(202) 400-3000<br>(202) 644-8099 – facsimile<br>charles.berardesco@nerc.net<br><br>Jim Robb*<br>Chief Executive Officer<br>Western Electricity Coordinating Council<br>155 North 400 West, Suite 200<br>Salt Lake City, UT 84103<br>(801) 883-6853<br>jrobb@wecc.biz | Sonia C. Mendonça*<br>Associate General Counsel and<br>Senior Director of Enforcement<br>North American Electric Reliability Corporation<br>1325 G Street N.W.<br>Suite 600<br>Washington, DC 20005<br>(202) 400-3000<br>(202) 644-8099 – facsimile<br>sonia.mendonca@nerc.net<br><br>Edwin G. Kichline*<br>Senior Counsel and Associate Director,<br>Enforcement Processing<br>North American Electric Reliability Corporation<br>1325 G Street N.W.<br>Suite 600<br>Washington, DC 20005<br>(202) 400-3000<br>(202) 644-8099 – facsimile<br>edwin.kichline@nerc.net<br><br>Chris Luras*<br>Director of Compliance Risk Analysis & Enforcement<br>Western Electricity Coordinating Council<br>155 North 400 West, Suite 200<br>Salt Lake City, UT 84103<br>(801) 883-6887<br>(801) 883-6894 – facsimile<br>CLuras@wecc.biz |

| | |
|---|---|
| Constance White*<br>Vice President of Compliance<br>Western Electricity Coordinating Council<br>155 North 400 West, Suite 200<br>Salt Lake City, UT 84103<br>(801) 883-6885<br>(801) 883-6894 – facsimile<br>CWhite@wecc.biz<br><br>*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. | Ruben Arredondo*<br>Senior Legal Counsel<br>Western Electricity Coordinating Council<br>155 North 400 West, Suite 200<br>Salt Lake City, UT 84103<br>(801) 819-7674<br>(801) 883-6894 – facsimile<br>rarredando@wecc.biz |

**Conclusion**

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

Respectfully submitted,

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

*/s/ Edwin G. Kichline*
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
Associate General Counsel and
Senior Director of Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments