November 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 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 of NERC Reliability Standards. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of two hundred thousand dollars ($200,000), in addition to other remedies and

[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).

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 WECC 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	VRF/ VSL	Discovery Method*	Penalty Amount
WECC2013012023	CIP-003-3	R5	Lower/ Severe	SC	$200,000
WECC2014013497	CIP-003-3	R6	Lower/ Moderate	SC	
WECC2012011467	CIP-005-1	R1	Medium/ Severe	SR	
WECC2013012367	CIP-005-3a	R5	Lower/ Severe	SC	
WECC2013012368	CIP-006-1	R1	Medium/ Severe	SC	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Penalty Amount
WECC2013012025	CIP-006-3c	R4	Medium/ Severe	SC	$200,000
WECC2012011598	CIP-006-3c	R5	Medium/ Severe	SR	
WECC2014013498	CIP-007-3a	R1	Medium/ Severe	SC	
WECC2014013658	CIP-007-3a	R2	Medium/ Severe	CA	
WECC2013012369	CIP-007-3a	R3	Lower/ Severe	SC	
WECC2012011599	CIP-007-1	R5	Medium/ Severe	SR	
WECC2014013499	CIP-007-3a	R5	Medium/ Severe	SC	
WECC2013012370	CIP-007-3a	R9	Lower/ High	SC	
WECC2014013500	CIP-007-3a	R9	Lower/ High	SC	
WECC2013012029	CIP-009-1	R1	Medium/ Severe	SC	

WECC2013012023 CIP-003-3 R5 - OVERVIEW

WECC determined that URE did not verify annually the list of personnel responsible for authorizing access to protected information. WECC determined the violation included seven individuals working within URE's various departments.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). As a result of URE's failure, unauthorized individuals may have had access to sensitive information. The potential risks associated with this violation were, however, limited due to URE's additional procedures. URE completed a review and promptly remediated the violation. URE has a limited number of individuals authorized to grant access to protected information; thus, any attempts by others to grant access to protected information would have been promptly discovered. Finally, when URE verified the list, the list remained the same and no employee was removed or added.

WECC determined the duration of the violation was one calendar year and resolved when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT009349 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. update the CIP-003 access procedure;
2. review the access list and record it in the review history section of the documentation;
3. implement a review form to record future annual reviews; and
4. schedule a calendar reminder to begin the review and to submit the appropriate documentation no later than December 30th of each year.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2014013497 CIP-003-3 R6 - OVERVIEW

WECC determined URE upgraded firmware and that URE failed to implement its Change Control and configuration management program across a subset of devices within URE's critical facilities while upgrading the firmware.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Because the firmware upgrade was not tested prior to installation, the firmware patch could have enabled ports and services or created unauthorized user accounts. Although URE failed to perform security testing prior to installing firmware upgrades, URE did implement preventive controls. Specifically, all of the relays in scope are located within Physical Security Perimeters (PSPs) and Electronic Security Perimeters (ESPs). URE monitors physical and logical access to the PSPs and

ESPs. URE also restricts access to authorized personnel with background checks and training on proper handling of the devices. URE placed the relays in protected networks with hardened boundary devices.

WECC determined the duration of the violation was from the time URE upgraded the firmware, to when URE followed its Change Authorization and Configuration Management protocol for the devices in scope.

URE submitted its Mitigation Plan designated WECCMIT011627 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. grant change authorization for the devices;
2. perform all security testing pursuant to CIP-007-3 R1;
3. implement job plan templates that include a notice to complete CIP-related tasks as part of computer-based work orders;
4. document and implement a process for adding new CIP equipment as it relates to system planning and automation; and
5. provide training on the new job plan and process document to applicable employees.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2012011467 CIP-005-1 R1- OVERVIEW

URE reported that it conducted a Cyber Vulnerability Assessment (CVA) and identified devices that should have been classified and protected as non-critical Cyber Assets.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Although URE did not meet the requirements of this Standard, URE did minimize the potential risks associated with this violation. Specifically, URE ensured that all devices involved in the violation were physically and electronically protected from unauthorized access 24 hours a day 7 days a week. Additionally, all URE personnel with access to the devices had undergone personnel risk assessments (PRAs) and had received CIP training. Finally, any actual access to the devices was monitored 24 hours a day 7 days a week.

WECC determined the duration of the violation to be from when URE was required to demonstrate compliance with this Standard through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT009590-2 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. remove the two IP connections for the management interfaces of the taps from the ESP;
2. relocate the connections to the unregulated quality assurance system;
3. provide the necessary protections to meet compliance and provide all relevant evidence. URE updated the CIP asset list to reflect the Cyber Assets' new designation, which is as both a Critical Cyber Asset (CCA) and an Electronic Access Control and Monitoring device (EACM);
4. submit a Technical Feasibility Exception request for the devices;
5. upgrade those authentication manager servers to the latest platform and perform a CVA on them prior to production; and
6. update the security operations recovery plan to include processes and procedures for the backup and storage of information required to successfully restore the EACM devices.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012367 CIP-005-3a R5 - OVERVIEW

WECC determined that URE failed to review, maintain, and update all documentation required by CIP-005-3a. WECC also determined that URE failed to update, within 90 calendar days, its ESP diagram when it decommissioned certain devices.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure increased the likelihood that changes in its network would go unnoticed and improper information about the network would be communicated to URE employees and contractors. The potential risks associated with this violation however, were limited due to URE's additional action of reviewing documentation in the years before and after the failure.

WECC determined the duration of the violation to be from when URE failed to review and update its documentation through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT009383 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. review documents and procedures referenced in Standard CIP-005-3;

2. update CIP-005 R5 documentation review procedure;
3. update the ESP diagram to remove the decommissioned asset; and
4. update the CIP master asset List to remove the decommissioned asset.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012368 CIP-006-1 R1 - OVERVIEW

WECC determined URE failed to provide node controllers the protections of CIP-007 R1, R2, R4, R5, and R9. Additionally, WECC determined URE failed to perform an annual exercise of its workstation recovery plan and failed to annually test its workstation backup media as required by CIP-009 R2 and R5. Furthermore, WECC determined URE failed to document its patch assessments for certain servers.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Although URE failed to provide certain protections required by the Standard, URE did limit the potential risks associated with the violation by employing different compensating measures. Specifically, for the node controllers involved in the violation, URE protected the devices from unauthorized access, and all personnel with access were authorized and had undergone PRAs and received CIP training. Additionally, URE tested and deployed available patches to the devices in scope.

WECC determined the duration of the violation was from the date the Standard became mandatory and enforceable, to when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT009349 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. schedule work with the application service vendors to complete full implementation of CIP controls;
2. perform the review of the recovery plan for the workstation;
3. perform the testing on the workstation backup media;
4. create an annual assessment calendar; and
5. provide training to all relevant group members.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012025 CIP-006-3c R4 - OVERVIEW

URE self-reported that at a substation PSP, on seven occasions, the access security badge reader was bypassed and the magnetic lock failed to operate as intended.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure created opportunities for individuals without authorization to access URE's PSPs and the CCAs located within the PSP. The potential risks associated with this violation, were however, limited due to URE's additional measures in place during the pendency of the violation. Specifically, the PSP in scope had alarm monitoring and a separate third-party monitoring alarm system. Additionally, the PSP is surrounded by a barbed wire fence and has a control gate with an alarm attached. Furthermore, the CCAs located within the PSP are fully monitored, and access is logged 24 hours a day 7 days a week.

WECC determined the duration of the violation to be from the first date the magnetic locks failed to open, to the last date the magnetic locks failed to operate.

URE submitted its Mitigation Plan designated WECCMIT011616 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. provide additional training to substation operations personnel regarding physical security at CIP substations; and
2. strengthen its overall approach to CIP security at the substations by designating security officers to regularly monitor alarms from the security system.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2012011598 CIP-006-3c R5 - OVERVIEW

URE reported that at a substation PSP, the security management system (SMS) reported a communication failure at its card readers. Because of the SMS outage, the substation PSP card readers were locked down and were not monitoring during the outage. URE reported that the outage continued for three days.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure created opportunities for individuals without authorization to access PSPs and the CCAs located within the PSP. The potential risks associated with this violation were, however, limited due to URE's additional measures in place during the pendency of the violation. Specifically, the PSP in scope had alarm monitoring and a separate third-party monitoring alarm system. Additionally, the PSP is surrounded by a barbed wire fence and has a control gate with an alarm attached. Furthermore, the CCAs located within the PSP are fully monitored, and access is logged 24 hours a day 7 days a week.

WECC determined the duration of the violation was from the date when the substation PSP experienced an SMS outage and monitoring failure, to when URE reestablished monitoring capability at the substation.

URE submitted its Mitigation Plan designated WECCMIT009373 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. review existing CIP documentation;
2. update corporate security procedures to include sufficient detailed instructions about how to respond to outages when the outage duration is longer than the 10-minute threshold for rebooting the system;
3. develop a new process and procedure that defines how the system will be used to address CIP-006 R5 as a secondary monitoring mechanism during outage situations; and
4. train personnel on the new procedures.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2014013498 CIP-007-3a R1 - OVERVIEW

WECC determined the URE implemented a firmware upgrade on relays at Critical Asset facilities. WECC determined the relays were not flagged as CIP-protected devices. Therefore, WECC determined URE did not conduct security testing prior to installing the firmware upgrade to ensure the firmware upgrades did not adversely affect existing cyber security controls.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. In this instance, URE failed to perform security testing prior to installing firmware upgrades on protective relays. This could negatively impact the existing cyber security controls on

these relays. Although URE failed to perform security testing prior to installing firmware upgrades, URE did implement detective controls. Specifically, all relays in scope are located within PSPs and ESPs. URE monitors physical and logical access to the PSPs and ESPs. URE also restricts access to authorized personnel with background checks and training on proper handling of the devices. URE placed the relays in protected networks with hardened devices. As a result, the relays were logically protected to allow traffic from only specific IP addresses and ports. These controls limit the vectors malicious personnel could use when attempting to compromise the devices.

URE also implemented detective controls. Specifically, URE had a control and monitoring network that would monitor and alarm if it detected a relay or breaker misoperation. URE implemented additional compensating controls. Specifically, prior to installing the patch in production, URE conducted functional testing in a test environment to test the effect of the change on the relays. By doing so, URE tested the patch to verify it would not break or damage the relay during installation.

WECC determined the duration of the violation was from the date URE upgraded the firmware, to when URE conducted post-testing to ensure there was no compromise of existing security controls.

To mitigate this violation, URE conducted post-testing to ensure there was no compromise of existing security controls. Based on the voluntary corrective actions taken by URE, WECC determined URE is not required to submit a Mitigation Plan for this violation.

WECC2014013658 CIP-007-3a R2 - OVERVIEW

URE directed WECC to use ports and services lists created for the annual CVA as baselines for its assessment during the Compliance Audit. WECC determined certain of these lists provided by URE lacked business justifications for the open ports and services. WECC also determined certain of URE's ports and services process documentation did not contain complete or updated lists of approved ports and services.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Failing to enable only ports and services required for normal and emergency operations could allow attackers to gain unauthorized access to the devices in scope. However, URE implemented certain compensating measures, including preventive and detective controls.

Specifically, all of the Cyber Assets reside behind electronic access points which restrict logical access to only authorized users. Additionally, all Cyber Assets physically reside within a PSP and are protected against unauthorized physical access. URE also employs intrusion detection, prevention, and antivirus

tools to detect and deter unauthorized access. These preventive and detective controls may prevent unauthorized individuals from gaining access or causing harm to the devices in scope

WECC determined the duration of the violation was from the first day of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011627 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. review its ports and services documentation to ensure that it is updated to reflect the current configuration of all CIP Cyber Assets; and
2. ensure that an appropriate business justification is identified for all open ports and services.

URE certified that its Mitigation Plan was completed.

WECC2013012369 CIP-007-3a R3 - OVERVIEW

WECC determined that URE became aware of new security patches or upgrades available for six EMS servers. WECC determined URE failed to adequately document the assessments of the applicability of security patches and security upgrades within 30 calendar days of availability in violation of CIP-007-3a R3.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to properly document its assessment security patches security upgrades increased the likelihood that its Cyber Assets may not be properly protected from potential cyber-attacks. The risks posed by URE's noncompliance were limited due to URE's additional protections. Specifically, URE assessed the security patches but failed to document that assessment as required by the Standard, thus the devices were up-to-date with appropriate protections. In addition, the EMS servers involved in the violation reside within a designated ESP. The ESP is monitored 24 hours a day, 7 days a week and produces active logs of activities that occur within the ESP.

WECC determined the duration of the violation was 30 calendar days after the release of the security patches, to when URE completed the assessment of the security patches.

URE submitted its Mitigation Plan designated WECCMIT009384 to address the referenced violations.

URE's Mitigation Plan required URE to update its procedures for its EMS and Windows patch assessment spreadsheet and assess patches that were missed.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2012011599 CIP-007-1 R5 - OVERVIEW

URE reported that it had one shared account, with access to EMS servers, which did not receive annual password changes. URE stated that the shared account was an emergency account and that it had never been used. URE also reported that devices at different locations did not have strong second-level passwords. URE reported that the second-level passwords had been changed from the factory default, but the passwords were not of sufficient strength to meet the requirements of CIP-007-1 R5.3.2.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to establish proper passwords and ensure that passwords are changed annually resulted in a situation where unauthorized access to the Cyber Assets could go unnoticed and unchecked. The potential risk associated with the violation was reduced due to URE's compensating measures.

URE had a strong password for the one shared account that was not changed annually. Additionally, all employees who had access to the one shared account had undergone PRAs and had comprehensive CIP training. Moreover, the EMS servers that were accessible from the one shared account generate activity logs that are actively monitored to ensure that only authorized individuals access the servers. URE also limited the potential risks associated with the devices that did not have strong second-level passwords. URE reported that each of the devices involved resides within a PSP and an ESP. Additionally, the devices were only accessible by certain personnel, each of whom had undergone PRAs and had received comprehensive CIP training. Moreover, the first-level passwords were strong passwords that met the complexity and length requirements of CIP-007-1 R5.

WECC determined the duration of the violation was from the date URE first failed to have strong second-level passwords on the devices, to when URE changed the second-level passwords on the devices.

URE submitted its Mitigation Plan designated WECCMIT009276-1 to address the referenced violation.

URE's Mitigation Plan required URE to:

1. change the emergency shared account password;

2. change the configuration of this account so that if the password is not changed within 90 days of use, the account password will automatically expire and require a reset prior to use; and
3. change the second-level passwords for the devices to strong passwords.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2014013499 CIP-007-3a R5 - OVERVIEW

WECC determined URE failed to change passwords at least annually on certain accounts in violation of CIP-007-3a R5.3.3. WECC determined three accounts had administrator access to the EMS domain workstations, one account had file transfer permissions to and from the open systems interconnection application, and the final account had local user access to the EMS workstations. WECC determined the workstations associated with the accounts are located at URE's system control center and backup control center.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE failed to change passwords at least annually on accounts. Failing to change passwords at least annually on these accounts could allow unauthorized individuals or individuals no longer authorized to have access to the devices in scope. However, in this instance URE had compensating measures and implemented preventive controls. Specifically, access to user accounts is managed through URE's account management tool. The tool ensures that only authorized individuals are granted access to EMS workstations and remote interactive access into the ESP is limited to individuals who require access. In addition, the shared account passwords at issue were known by a limited number of individuals and were not intended for human use.

WECC determined the duration of the violation was one year after URE last changed the passwords through completion of its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011638 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. change the passwords that will be reviewed each quarter by information technology department managers;
2. manage interactive access into the EMS environment account; and
3. remove the account from all CCAs on which it resides.

WECC2013012370 CIP-007-3a R9 - OVERVIEW
WECC determined that URE's departments failed to review CIP-007-3 documentation annually.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to perform an annual review on its CIP-007-3 documentation presented an opportunity where changes to the documents would not have been properly reflected and protections offered to CCA may not have been properly applied or removed. The potential risks associated with this violation were limited due to URE's additional procedures. Specifically, URE had conducted a review of the documentation in the previous year and, upon discovery of the possible violation, immediately conducted a review of its CIP-007-3 documentation.

WECC determined the duration of the violation began when URE failed to conduct the annual review and ended when URE reviewed the CIP-007-3 documentation.

URE submitted its Mitigation Plan designated WECCMIT009386 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. review the access list and record it in the review history section of the documentation;
2. review the documents;
3. update the CIP-007-3a R9 documentation review procedure;
4. create a calendar that lists all assessment activities that need to take place on a monthly, quarterly, and annual basis; and
5. train applicable group members on the new process.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2014013500 CIP-007-3a R9 - OVERVIEW
WECC determined that URE did not review its CIP-007-3 R4 antivirus document annually, in violation of CIP-007-3a R9.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Failing to review and update documentation could lead to personnel performing out of date or incorrect processes on the devices in scope. However, URE implemented preventive controls as compensating measures. URE tests significant changes to devices prior to deploying

changes. This would alert URE to any issues prior to the changes affecting the devices in scope. Additionally, URE updated its calendar spreadsheet for tracking the annual procedure reviews.

WECC determined the duration of the violation began when URE failed to review the antivirus document and ended when URE reviewed the antivirus document.

URE submitted its Mitigation Plan designated WECCMIT010931 to address the referenced violations.

URE's Mitigation Plan required URE to review the antivirus for EMS procedure.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012029 CIP-009-1 R1 - OVERVIEW

WECC determined URE failed to conduct one annual review of its EMS recovery plan. As a result, WECC determined URE was in violation of CIP-009-1 R1.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure increased the opportunity for its CCA to be rendered inoperable in the event of an emergency. The potential risks associated with the violation were limited due to additional protections in place during the pendency of the violation. Specifically, the EMS workstations involved in the violation were located within a defined ESP and PSP. Furthermore, URE monitors physical and logical access to the devices 24 hours a day 7 days a week. Finally, URE did have a partial recovery plan in place and had trained its operators on the recovery plan.

WECC determined the duration of the violation was for one calendar year.

URE submitted its Mitigation Plan designated WECCMIT009282-2 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. create a group annual assessment calendar that will list all assessment activities that need to take place on a monthly, quarterly, and annual basis;
2. revise the recovery plan to contain more detail on severity and duration and also include more detail for roles and responsibilities, including which departments to contact, what the role of each department is, and a contact phone number for each department; and
3. train all applicable group members on the new process.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two hundred thousand dollars ($200,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC 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 WECC considered a mitigating factor;
3. URE self-reported three of the violations;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations of WECC2013012023, WECC2014013497, WECC2013012368, WECC2013012367, WECC2013012025, WECC2012011598, WECC2014013498, WECC2014013658, WECC2013012369, WECC2012011599, WECC2014013499, WECC2013012370, and WECC2014013500 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. The violations of WECC2014013658, WECC2012011467, and WECC2013012368 posed a moderate risk but did not pose a serious or substantial risk to the reliability of the BPS;
7. URE agreed to implement Reliability Focused Terms;[4]
8. URE sent WECC a letter reporting on URE's successful progress in implementing the Reliability Focused Terms outlined in the Settlement Agreement; and
9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[4] URE committed to the following terms: 1) to strengthen preventive and detective controls to minimize human error associated with the performance of CIP compliance related tasks; 2) to engage an outside consultant to support URE's transition to CIP Version 5 by analyzing URE's CIP controls; 3) to report to WECC on its progress in these efforts by the end of second quarter of 2015; and 4) to complete the work pertaining to the above non-monetary sanctions no later than December 31, 2015.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of two hundred thousand dollars ($200,000) 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[5]

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, the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on October 1, 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 thousand dollars ($200,000) 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.

[5] *See* 18 C.F.R. § 39.7(d)(4).

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

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
Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz	Michael Moon* Vice President Entity Oversight Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7608 (801) 883-6894 – facsimile mmoon@wecc.biz
Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz	*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
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

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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council