December 30, 2013

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. NP14-_-000

Dear Ms. Bose:

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

This Notice of Penalty is being filed with the Commission because 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] of CIP-003, CIP-006, and CIP-007. According to the Settlement Agreement, URE agrees and stipulates to the facts of the violations, and has agreed to the assessed penalty of one hundred fifty thousand dollars ($150,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201102906, WECC201103022, WECC201002325,

[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 (2013). *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).

[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.

WECC201102498, WECC201102806, WECC201002358, and WECC201002328 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 executed on September 19, 2013, by and between WECC and URE, which is included as Attachment a. 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 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Western Electricity Coordinating Council	Unidentified Registered Entity	NOC-2234	WECC201102906	CIP-003-1	R4	Medium	$150,000
			WECC201103022	CIP-006-3c	R1: R1.4; R1.5	Medium	
			WECC201002325	CIP-006-1	R1	Medium	
			WECC201102498	CIP-006-1	R1: R1.1; R1.2; R1.4; R1.6; R1.8	Medium	
			WECC201102806	CIP-006-1	R3.1	Medium	
			WECC201002358	CIP-007-2a	R1	Medium	
			WECC201002328	CIP-007-1	R5: R5.2.1; R5.3.2	Medium	

CIP-003-1

The purpose statement of Reliability Standard CIP-003-1 provides in pertinent part: "Standard CIP-003 requires that Responsible Entities[4] have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

[Footnote added.]

WECC201102906 CIP-003-1 R4

CIP-003-1 R4 provides:

> Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
>
> > R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
> >
> > R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
> >
> > R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

CIP-003-1 R4 has a "Medium" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE submitted a Self-Report to WECC stating it had a violation of CIP-003 R4. WECC determined that URE failed to implement its physical security program to identify, classify, and protect information

[4] Within the text of Standard CIP-003, CIP-006, and CIP-007, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

associated with Critical Cyber Assets (CCAs) when a URE employee left a notebook containing Critical Assets lists, which should have been locked in a cabinet pursuant to URE's program, on a bookshelf in a manager's office.

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). URE has a documented program to protect CCA information, has a process for granting access to CCA information, and provides annual CIP training to all employees with access to CCAs. The notebook was left in a manager's office which was located within a restricted access area, on a floor requiring card access, limited to a small number of URE-only personnel.

CIP-006

The purpose statement of Reliability Standard CIP-006 provides in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

WECC201103022 CIP-006-3c R1: R1.4; R1.5

CIP-006-3c R1 provides in pertinent part:

> Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
>
> *****
>
> R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
>
> R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.

CIP-006-3c R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to WECC stating it had a violation of CIP-004 R4.2. While WECC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation. WECC determined the facts of the violation related to CIP-006-3c R1.4 and R1.5. WECC determined URE had four instances relating to a single violation of CIP-006 R1.

One URE security guard was granted physical access to four URE Physical Security Perimeters (PSPs). URE intended for the security guard to have access to only one of those four PSPs. The security guard had physical access for approximately 33 days to each of the four PSPs, although the security guard had no knowledge that he had access to the additional PSPs. Two of the PSPs were in the control center and contained the energy management system (EMS) workstations which are CCAs. The third PSP was in the backup control center and contains dispatch workstations which are CCAs. The three PSPs to which the security guard had improper physical access had CIP-005 and CIP-006 protections for the CCAs. Two of the PSPs were staffed 24 hours a day, seven days a week. All PSPs in scope are in secure facilities which required card reader access to gain entry. WECC determined the security guard's access card could have been used to gain such entry. As a result, WECC determined URE had a violation of CIP-006 R1.5 because URE did not review access authorization requests in accordance with CIP-004-3 R4.

A separate but similar incident occurred when access to two PSPs was inadvertently added to the wrong contract worker's badge. The error was caught, and access was removed within two minutes of access being added incorrectly.

On two separate occasions, proper procedures were not followed when entering a PSP. The first incident occurred when one individual with authorized physical access gained entry to a PSP without using the card access reader. The individual followed another authorized employee into the PSP. URE has video recording at the PSP access point; the video did record the individual entering the PSP without using the card access reader. The PSP houses EMS workstations (which URE identified as CCAs). By following an individual through an open door, the individual in scope of this violation circumvented controls outlined in CIP-006 R4.

A second incident occurred when one employee tailgated another employee into a PSP without swiping his access badge. The employee realized that he did not enter the PSP correctly, and both employees immediately exited the PSP and re-entered by swiping their badges correctly. In both instances, the personnel were authorized for access but did not follow proper procedure when entering the PSPs.

WECC determined the duration of the violation to be from the date of the first instance, 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 security guard in the first instance had current CIP training and a current personnel risk assessment (PRA). The additional three PSPs for which the guard did not have authorization were staffed continuously, and CCAs were located within PSPs and Electronic Security Perimeters (ESPs) with CIP-005 and CIP-006 protections, including continuous logging and monitoring of physical and electronic access. The PSPs in scope are in secure facilities which require card reader access and have video recording mechanisms in place. In the second instance, the error was caught, and access was removed within two minutes of it being added incorrectly. In both the third and fourth instances, the personnel were authorized for access but did not follow proper procedure when entering the PSPs. In the fourth instance, the security guard realized immediately that he did not enter the PSP correctly, exited the PSP, and re-entered by swiping his badge correctly.

The short duration of the instances, and immediate corrections of the violations, indicated that URE had good systems in place that employees followed. The reported instances are isolated instances which were responded to quickly and appropriately.

WECC201002325 CIP-006-1 R1

CIP-006-1 R1 provides in pertinent part:

> Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.
> >
> > *****
> >
> > R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually

CIP-006-2 R1.6 and R1.8 provide:

> Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
>
> R1.6. Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.
>
> *****
>
> R1.8. Annual review of the physical security plan.

CIP-006-2 R2.2 provides:

> R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
>
> *****
>
> R2.2. Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.

CIP-006-1 R1.6 has a "Medium" VRF and a "Severe" VSL. CIP-006-1 R1.8 and R1.9 have "Lower" VRFs.

URE submitted Self-Reports to WECC stating it had a violation of CIP-006-2 R2. While WECC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation. WECC reviewed the Self-Reports and determined each Self-Report identified a narrow scope of a broader violation, but did not identify multiple violations.

URE failed to ensure that its physical security plan was reviewed at least annually as required by CIP-006-2 R1.8.

URE did not provide continuous escorted access within the PSP of personnel not authorized for unescorted access as required in CIP-006-2 R1.6. Specifically, URE allowed one unauthorized contract worker to gain physical access to the grid operations control center, and one contract worker, without permission to act as an escort, escorted two individuals (the contract worker's children) into a distribution control center that contained CCAs.

URE did not afford a Cyber Asset used in the access control and monitoring of the PSP the protective measures specified CIP-003 R4, and a different Cyber Asset used in the access control and monitoring of the PSP the protective measures specified in CIP-009 R1, as required by CIP-006-2 R2.2.

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 moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to review and approve a physical security plan and failing to provide continuous escorted access could lead to URE's Cyber Assets within PSPs being unprotected, unmonitored, or unchecked, and therefore could allow unauthorized physical access to CCAs within the PSP. Failing to document and implement a program to ascertain and distinguish information related to CCAs could cause URE personnel to be unaware of the content or location of such information, which could result in the information being misused.

URE did have a physical security plan which included controls (e.g., physical access, monitoring physical access, and logging physical access) and provided the CCAs with the protective measures required in CIP-006. URE personnel conducted the review of the physical security plan, but did not formalize the review with a signature.

URE staffs its controls centers 24 hours a day, seven days a week; thus URE personnel were present, although not escorting the visitors. URE logs and monitors its control centers 24 hours a day, seven days a week, for any physical and electronic access; the EMS workstations in the control center require usernames and passwords for access; universal serial bus (USB) ports on the CCAs are disabled; keyboard, video, and mouse (KVM) switches, that are used to control the workstations, are behind a locked door; and only the necessary ports and services are enabled on the Cyber Assets in the control center.

URE: 1) had continuous electronic and physical logging and monitoring at its PSPs; 2) used an active directory group to limit access to the access control and monitoring server in scope; 3) used access points to ESPs to protect from outside electronic access; and 3) had an intrusion detection system (IDS) that monitors electronic access in the ESP from outside access.

WECC201102498 CIP-006-1 R1: R1.1; R1.2; R1.4; R1.6; R1.8

CIP-006-1 R1 provides in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
> >
> > R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.
> >
> > *****
> >
> > R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
> >
> > *****
> >
> > R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.
> >
> > *****
> >
> > R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005

Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

CIP-006-1 R1, R1.1, R1.2, R1.4, and R1.6 have "Medium" VRFs and a "Severe" VSL. CIP-006-1 R1.8 has a "Lower" VRF.

URE submitted Self-Reports to WECC stating it had a violation of CIP-006-1 R1. While WECC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation. WECC reviewed the Self-Reports and determined each Self-Report identified a narrow scope of a broader violation, but did not identify multiple violations.

URE failed to afford 16 access control and monitoring (ACM) workstations, which could be used to authorize access to URE's PSPs, the protections of CIP-006-1 R2 and R3; CIP-007-1 R1, R2, R5, R6, R8, and R9; CIP-008-1 R1 and R2; CIP-009-1 R1, R2, R3, R4, and R5. Two additional servers used to manage URE's badge reader system were not afforded the protections of CIP-003 R4 and CIP-007 R1.

URE failed to establish a six-wall perimeter for two PSPs, and failed to identify two egress-only doors as access points at two other PSPs.

URE reported six instances where visitor escort procedures were not followed properly and one instance where an authorized employee entered a PSP but failed to badge into the PSP correctly.

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 moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, deficiencies in a PSP could lead to Cyber Assets within that PSP being unprotected, unmonitored, or unchecked, or allow for unauthorized physical access to CCAs within that PSP. Such access could be used to cause harm to CCAs essential to the operation of the BPS.

The violation extended across a range of physical access issues which presented numerous opportunities for unintentional or malicious physical access. Where the PSPs did not have sufficient six-walled protections, the PSP was itself inside another PSP that included the necessary protections.

Where URE did not identify egress doors as access points, the doors were alarmed or monitored continuously by URE's security personnel. URE logs and monitors its control centers 24 hours a day,

seven days a week, for any physical and electronic access; the EMS workstations in the control center require usernames and passwords for access; USB ports on the CCAs are disabled; KVM switches, that are used to control the workstations, are behind a locked door; and only the necessary ports and services are enabled on the Cyber Assets in the control center.

URE: 1) had continuous electronic and physical logging and monitoring at its PSPs; URE 2) used an active directory group to limit access to the access control and monitoring server in scope; 3) used access points to ESPs to protect from outside electronic access; 3) had an IDS that monitors electronic access in the ESP from outside access; and 4) URE personnel and contractors with access to the devices at issue had current PRAs and CIP cyber security training.

WECC201102806 CIP-006-1 R3.1

CIP-006-1 R3 provides in pertinent part:

> R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:
>
> > R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

CIP-006-1 R3.1 has a "Medium" VRF and a "High" VSL.

URE submitted a Self-Report to WECC stating it was in violation of CIP-006-1 R3.1. URE failed to finalize installation for an alarm system at a single access point to one PSP. The access point could not generate "door forced open" and "door held open" alarms.

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 monitored this access point with video recording 24 hours a day, seven days a week. The card reader and the card access control system did record and log all "Access Denied" and "Access Granted" events and therefore appropriately logged physical access. The PSP is in a secured

facility that restricts access with badge readers, and all access points to the facility are monitored by video recording.

CIP-007

The purpose statement of Reliability Standard CIP-007 provides in pertinent part:

> Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

WECC201002358 CIP-007-2a R1

CIP-007-2a R1 provides:

> Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
>
> > R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.
> >
> > R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
> >
> > R1.3. The Responsible Entity shall document test results

CIP-007-2a R1 has a "Medium" VRF and a "High" VSL.

URE submitted a Self-Report to WECC stating it was violation of CIP-007 R1. URE failed to test patches for one EMS workstation prior to applying the patches.

URE has a development environment for testing changes and patches prior to moving the systems into the production environment. All the Cyber Assets in the development environment have been

configured as a member of the development group and automatically receive changes and patches for testing. The one EMS workstation was then moved to the production network; however, URE did not change the configuration setting that defined the EMS workstation as a member of the "development group" to the "production group." As a result, the EMS workstation (moved from the development group to the production environment) received the June and July patches before these patches were tested. Therefore, URE failed to implement and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

WECC determined the duration of the violation to be from when the EMS workstation moved from the development group to the production group, through when URE implemented the patches and appropriately updated its production system.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. One out of nine EMS workstations received the patches before testing was complete; the other eight EMS workstations on the network had current antivirus and anti-malware software and only enabled those ports and services necessary; none of the workstations had USB drives. The facility and network in scope have 24 hour a day, seven day a week logging and monitoring of physical and electronic access controls. The EMS workstations have a redundant system ready for operation if the primary workstation should fail. URE has backup and restore procedures, as required in CIP-009, which would allow URE quickly to restore and bring back online any EMS workstation.

WECC201002328 CIP-007-1 R5: R5.2.1, R5.3.2

CIP-007-1 R5 provides in pertinent part:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> *****
>
> R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
>
> R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

*****

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

*****

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

CIP-007-1 R5.2.1 has a "Medium" VRF and a "Severe" VSL. CIP-007-1 R5 and R5.3.2 have a "Lower" VRF.

URE submitted a Self-Report to WECC stating that it had a violation of CIP-007-1 R5. Two devices that URE classified as CCAs had a default system password for accessing the configuration of the devices. The devices were located in the data center on URE's EMS network and were in service prior to the Standard's compliance date.

Subsequently, WECC submitted a data request to URE to verify that URE implemented new passwords on the devices. In its response to the data request, URE stated that the changed passwords met CIP-007-1 R5.3.1 and CIP-007-1 R5.3.3, but did not use "special" characters as required in CIP-007-1 R5.3.2. WECC determined this failure increased the scope of the original self-reported violation.

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 two CCAs are located in an ESP and PSP and have the protective measures required by CIP-005 and CIP-006. The CCAs have 24 hour a day, seven days a week logging and monitoring of physical and electronic access controls, physical security controls to access the data center, and electronic security controls.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred fifty thousand dollars ($150,000) 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 its penalty determination. WECC also determined, however, that URE's rigorous self-assessments and commitment to prompt self-reporting, coupled with URE's internal compliance program, led to URE's detection and reporting of these violations. WECC considered URE's compliance culture such that the set of repeat violations herein do not warrant the full aggravation usually assessed for multiple violations resulting from the same or similar conduct;
2. URE self-reported the violations;
3. URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violations, which WECC considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations 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 fifty thousand dollars ($150,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[5]

WECC201102906 CIP-003-1 R4

URE's Mitigation Plan to address its violation of CIP-003-1 R4 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT006496 and was submitted as non-public information to FERC in accordance with FERC orders.

[5] *See* 18 C.F.R § 39.7(d)(7).

URE's Mitigation Plan required URE to:

1. Update its CCA information program to specify accurately what information needs to be restricted. URE posted this on an internal website and emailed the program to applicable personnel;
2. Place the Critical Asset list at issue in a locked container;
3. Have the individual associated with this violation attend training and attend a meeting related to URE drafting its updated information protection program;
4. Perform internal assessments on information program compliance; and
5. Conduct annual training on the updated program.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Revised CCA information program documentation;
2. Copy of company-wide communication (email) to all employees with CCA physical access notifying them of revised CCA information protection program; and
3. List of employees notified of changes.

WECC verified that URE's Mitigation Plan was completed.

WECC201103022 CIP-006-3c R1: R1.4; R1.5

URE's Mitigation Plan to address its violation of CIP-006-3c R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT006498 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Update the physical security department's PSP secondary verification process. The secondary verification process is used to verify that requested physical access additions, modifications, or removals are completed correctly. The secondary verification process is performed by a member of the physical security department other than the member adding, modifying, or removing the requested physical access;

2. Update URE's documented process to require finishing an in-process item before moving on to a new item (to reduce or minimize the chance that human error will continue to pose problems);
3. Notify, by email, applicable employees about the updated procedures;
4. Conduct a meeting between the employee at issue in the second instance of the violation and the management leader for future prevention ideas, and have the employee and work group attend a training session on how properly to enter and escort in a restricted area;
5. Add signage at its physical access points regarding compliant and appropriate protocols;
6. Train all personnel within the physical security department who have administration rights to the URE card access application; and
7. Conduct a meeting between URE's regulatory compliance department and the employees involved in this violation to review guidance for visitor management. URE's regulatory compliance department also stressed the importance of not assuming the employees have physical access to CIP restricted areas. Specifically, URE stated in the mitigation plan "if employees are unsure what CIP restricted areas they have physical access to, they should contact their supervisor or a member of the physical security department to inquire prior to attempting to access a CIP restricted area."

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Evidence (meeting request screen shot) of corrective interview conducted with employee who did not swipe access card to enter PSP;
2. Revised card access procedure;
3. PSP access grant review process;
4. Copy of participant log for scenario-based CIP access training session;
5. Image of updated signage posted outside PSP access point;
6. Copy of email sent by the manager to all individuals with access to the PSP at issue;
7. Copy of email sent by manager to all operators regarding the PSP access procedures;
8. Email to all employees in physical security department from the manager. The email specifies that individuals making updates to card access need to ensure that only one cardholder account is open at any one time;
9. Email detailing revised the CCA visitor procedure; and

10. Company communications (email) detailing revisions in revised CCA visitor procedures.

WECC verified that URE's Mitigation Plan was completed.

WECC201002325 CIP-006-1 R1

URE's revised Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to WECC.[6] The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as MIT-10-3221-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Assign the physical security plan to the appropriate senior manager for review and approval;
2. Discuss the corporate policies for physical access controls and expectations as an escort when allowing an employee or contract worker that does not have authorized unescorted physical access into a CCA area with those involved;
3. Send a reminder email to all affected employees concerning the corporate policy for physical access controls from the Standard;
4. Discuss as a "lessons learned" opportunity during the August monthly dispatcher meeting. Discussion included an overview of the corporate policy and the requirements of the CIP cyber security Standard. URE took similar measures, i.e., training, written and verbal reminders, with its contracted vendors;
5. Remove IP addresses from the configuration details from databases associated with URE's ACM devices to ensure information associated with URE's ACM devices is protected in accordance with URE's information program pursuant to CIP-003 R4; and
6. Add language to its card access system recovery plan to address the requirements of CIP-009.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. URE's physical security plan;
2. URE's updated physical security plan procedures;

[6] URE initially submitted a Mitigation Plan for each of its Self-Reports. The original Mitigation Plan for this violation ID was filed with FERC as MIT-10-3221. Later, URE submitted a comprehensive Mitigation Plan that superseded and replaced the individual plans.

3. URE's updated escort procedures;
4. Notes from URE's lessons learned meetings; and
5. Other training materials and disciplinary action materials.

WECC verified that URE's Mitigation Plan was completed.

WECC201102498 CIP-006-1 R1: R1.1; R1.2; R1.4; R1.6; R1.8

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT005989 and was submitted as non-public information to FERC in accordance with FERC orders.[7]

URE's Mitigation Plan required URE to:

1. Reduce the number of ACM workstations from 16 to two, and add protections of CIP-006-3 R2.2 to the two ACM workstations that authorize access to PSPs;
2. For the two servers in scope of the violation, remove and delete sensitive information from the infra change management system, change IP addresses of devices that were exposed, and change URE processes to include placing sensitive information (e.g., IP addresses) in secure areas such as a password vault;
3. Document and create new ACM testing procedures in accordance with CIP-007 R1 and train its personnel regarding the update to testing procedures;
4. For the four PSPs in scope, add a mesh extension to the top of one PSP and add a tamper alarm to a window. Regarding the door in scope, disable the door so it no longer could be opened from the interior or exterior. Reduce the size of a PSP so the door in question no longer is an access point to the PSP. Secure the floor panels by inserting screws on the top and bottom of all four corners of the floor panel;
5. Train its personnel on applicable and appropriate password complexity policy and install a technical control for enforcing password complexity;
6. Update its cyber security policy to better address CIP-007 R5 and modify the passwords in scope to meet the requirements of CIP-007 R5;

[7] Due to an administrative error, NERC did not timely submit the subject Mitigation Plan to FERC.

7. Update documentation of required ports and services and develop a new process for identifying required ports and services;
8. Create and implement a new cyber vulnerability assessment procedure specifically for the servers related to this violation, create a spreadsheet to track CIP-007 documentation that requires annual review, move oversight and management of the servers to the corporate security department, and implement a patch to correct a bug that prevented logging;
9. Implement security information and event management alerting to alert when logs are not being reported to the server;
10. Notify, through email, all employees with authorized access and make the employees aware of the appropriate procedures regarding escorting personnel in CIP-protected areas, and train all employees with authorized access regarding the URE rules of escorting; and
11. Train its effected employees on proper access procedures given to all employees with authorized access to CCAs.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Work order to uninstall client software on eight virtual workstations;
2. Pictures of the new secure server rack;
3. Card access virtual environment diagram;
4. PACs electronic control procedures;
5. Revised CIP Standards policy sections on password complexity;
6. Communications regarding password complexity to employees and contractors who have access to PACs systems;
7. Meeting material held by IT staff on password complexity;
8. Copy of Critical Asset authorized ports and services process;
9. Copies of dynamic port ranges and updated baseline reports for access control and monitoring of services;
10. Updated procedures used to ensure only ports and services required for normal and emergency operations are enabled on ACM systems;
11. Revised procedure to ensure vulnerability assessment is performed for access servers;
12. A copy of card access CIP documentation spreadsheet;

13. A copy of the revised documentation review procedures;
14. Email detailing completed work requests for PSPs;
15. Copies of completed work requests for PSPs;
16. Security information and event management logs;
17. Copy of URE's NERC continuing education program;
18. Copy of CIP-006 training material;
19. Class rosters for training;
20. Control center tours;
21. Corporate communication to all employees involved in the event- on security;
22. Power Point presentation given to all employees authorized for unescorted PSP access;
23. Additional CIP training course;
24. CIP training acknowledgement;
25. CIP test with answers highlighted;
26. Memo of updated mobile patrol post orders;
27. Affidavit from IT attesting to mitigation;
28. Patch change request documentation;
29. Service request tickets; and
30. Monthly Patch application process and logs for ACM servers.

WECC verified that URE's Mitigation Plan was completed.

WECC201102806 CIP-006-1 R3.1

URE's Mitigation Plan to address its violation of CIP-006-1 R3 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT005778 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Correct the wiring oversight for the door at issue in the violation; and

2. Verify that the card reader was functioning correctly and the door appropriately generates each of the four door event types when tested.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. A work request;
2. A document with the four alarm types listed;
3. Interviews confirming the access point triggered the four door alarm types;
4. A document demonstrating the configuration of multiple access points with the included missing alarm triggers, specifically supporting that the physical security analyst added a trigger to each of seven "Access Denied" event types not initially included in URE's default group of event triggers; and
5. A document supporting that missing triggers were configured appropriately.

WECC verified that URE's Mitigation Plan was completed

WECC201002358 CIP-007-2a R1

URE's Mitigation Plan to address its violation of CIP-007-2a R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT005989 and was submitted as non-public information to FERC in accordance with FERC orders.[8]

URE's Mitigation Plan required URE to:

1. Change the EMS workstation's configuration to the production group;
2. Configure all the workstations on the EMS network to monitor the EMS network workstations configuration changes related to software patches; and
3. Conduct a one-on-one meeting with the technician involved with the violation.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. A screen shot depicting that the workstation is located in the production group of workstations;

[8] Due to administrative error, NERC did not timely submit the subject Mitigation Plan to the Commission.

2. A report that alerted an URE EMS analyst (i.e. an exception report that shows changes that were made to the workstation that were not yet part of the security baseline); and
3. A summary of workstation baseline results.

WECC verified that URE's Mitigation Plan was completed.

WECC201002328 CIP-007-1 R5: R5.2.1, R5.3.2
URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as MIT-09-3750 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Change the default passwords for the two servers and update the passwords to contain special characters;
2. Train the employee who entered the wrong password; and
3. Provide training to the EMS leader on appropriate password controls.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Two .pdf documents showing the password changes; and
2. An email stating that the employee who entered the wrong password and the EMS leader were trained on the password controls.

WECC verified that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[9]

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,[10] the

[9] *See* 18 C.F.R. § 39.7(d)(4).
[10] *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

NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2013. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred fifty thousand dollar ($150,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of 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 considered the following factors:

1. WECC considered URE's compliance history as an aggravating factor in its penalty determination, as discussed above;
2. URE self-reported the violations;
3. WECC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violations which WECC considered a mitigating factor, as discussed above;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred fifty thousand dollars ($150,000) 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

The attachments to be included as part of this Notice of Penalty are the following documents:

¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

a) Settlement Agreement by and between WECC and URE executed September 19, 2013, included as Attachment a;

b) Record documents for the violation of WECC201102906 CIP-003-1 R4, included as Attachment b:

   1. URE's Source Document;
   2. URE's Mitigation Plan designated as WECCMIT006496;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

c) Record documents for the violation of WECC201103022 CIP-006-3c R1: R1.4; R1.5, included as Attachment c:

   1. URE's Source Document;
   2. URE's Source Document;
   3. URE's Mitigation Plan designated as WECCMIT006498;
   4. URE's Certification of Mitigation Plan Completion;
   5. WECC's Verification of Mitigation Plan Completion;

d) Record documents for the violation of WECC201002325 CIP-006-1 R1, included as Attachment d:

   1. URE's Source Document dated;
   2. URE's Source Document dated;
   3. URE's Mitigation Plan designated as MIT-10-3221-1;
   4. URE's Certification of Mitigation Plan Completion;
   5. WECC's Verification of Mitigation Plan Completion;

e) Record documents for the violation of WECC201102498 CIP-006-1 R1: R1.1; R1.2; R1.4; R1.6; R1.8, included as Attachment e:

   1. URE's Source Document;
   2. URE's Source Document;
   3. URE's Mitigation Plan designated as WECCMIT005989;
   4. URE's Certification of Mitigation Plan Completion;
   5. WECC's Verification of Mitigation Plan Completion;

f) Record documents for the violation of WECC201102806 CIP-006-1 R3.1, included as Attachment f:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT005778;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

g) Record documents for the violation of WECC201002358 CIP-007-2a R1, included as Attachment g:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT005989;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

h) Record documents for the violation of WECC201002328 CIP-007-1 R5: R5.2.1, R5.3.2, included as Attachment h:

1. URE's Source Document;
2. URE's Mitigation Plan designated as MIT-09-3750;
3. URE's Certification of Mitigation Plan Completion; and
4. WECC's Verification of Mitigation Plan Completion.

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 213-2673 (801) 582-3918 – facsimile Mark@wecc.biz Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6855 (801) 883-6894 – facsimile CWhite@wecc.biz	Sonia C. Mendonça* Assistant General Counsel and 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 Edwin G. Kichline* North American Electric Reliability Corporation Senior Counsel and Associate Director, Enforcement Processing 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Chris Luras* Director of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@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/ Sonia Mendonça

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

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

Sonia C. Mendonça
Assistant General Counsel and 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

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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments