PRIVLIEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

March 31, 2014

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 (URE)
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-002-2 R3; CIP-005-3 R1 and R5; CIP-006-1 R1, R2 and R3; and CIP-007-1 R1 and R2. According to the Settlement Agreement, URE agreed and stipulated to the terms of the Settlement Agreement, and has agreed to the assessed penalty of four hundred sixty-five thousand dollars ($465,000), 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 WECC2012011042, WECC2012011043, WECC2012011044,

[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.

WECC2012011140, WECC2012011053, WECC2012011054, WECC2012011058 and WECC2012011059 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	URE	NOC-2205	WECC2012011042	CIP-002-2	R3	High	$465,000
			WECC2012011043	CIP-005-3	R1	Medium	
			WECC2012011044	CIP-005-3	R5	Lower	
			WECC2012011140	CIP-006-1	R1	Medium	
			WECC2012011053	CIP-006-1	R2	Medium	
			WECC2012011054	CIP-006-1	R3	Medium	
			WECC2012011058	CIP-007-1	R1	Medium	
			WECC2012011059	CIP-007-1	R2	Medium	

CIP-002-2 R3
The purpose statement of Reliability Standard CIP-002-2 provides:

NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-002-2 R3 provides:

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

CIP-002-2 R3 has a “High” Violation Risk Factor (VRF) and a “High” Violation Severity Level (VSL).

WECC performed an on-site Compliance Audit (Audit) of URE. WECC's Audit Team reviewed URE's Risk Based Assessment Methodology (RBAM) and associated lists of Critical Assets and Critical Cyber Assets (CCAs). In addition, WECC's Audit Team conducted facility site tours to confirm specific listings of CCAs. During the site tours, WECC's Audit Team identified nine discrepancies on URE's CCA lists.

WECC reviewed the Audit findings and determined that URE was in violation of CIP-002-2 R3 for failing to update its CCA lists when changes to these assets occurred. Specifically, URE's lists represented an inaccurate depiction for nine CCAs that have been removed from service, have been misidentified, or have been identified incorrectly on the CCA list.

WECC determined the duration of the violation to be from the date the first CCA was removed from service, through the date URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, the risk to the BPS was moderate because URE's failure to update the list of CCAs, as necessary, rendered these devices vulnerable to cyber attacks or misuse. The assets were located across five substations and the discrepancies occurred because URE's asset strategists failed to follow URE's validation process when changes occurred. WECC determined that URE's failure to confirm that corrections to the list are made and actions are recorded within its equipment validations process represents weak asset management practices. The risk was mitigated by the fact that URE afforded a number of protective measures to the nine CCAs at issue. Specifically, all the devices were physically secure and located within a Physical Security Perimeter (PSP). Physical access to the devices was limited to individuals who had Personnel Risk Assessments (PRAs) and cyber security training. Finally, physical and electronic access was logged and monitored and unauthorized access attempts would have triggered alarming to notify URE staff.

CIP-005-3 R1.5 and R1.6

The purpose statement of Reliability Standard CIP-005-3 provides: "Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-005-3 R1 provides in pertinent part:

> R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

> R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.
>
> R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

CIP-005-3 R1 has a "Medium" VRF and a "Severe" VSL.[4]

During URE's Audit, WECC's Audit Team reviewed URE's network diagrams, documentation of Critical and non-critical Cyber Assets within URE's Electronic Security Perimeters (ESPs), all electronic access points to the ESPs, and the Cyber Assets deployed for the access control and monitoring of these access points. In addition, the Audit Team conducted facility site tours to confirm specific listings of assets. During the site tours, the Audit Team identified several access control and monitoring assets that were not identified in URE's network diagrams. For approximately 60 assets URE did not classify the devices as access control and monitoring devices. URE only took into consideration access points and failed to consider assets that control or log access. Because URE failed to identify these assets as access control and monitoring assets, it did not afford the protective measures specified in CIP-005-3 R1.5 to these assets.

WECC reviewed the Audit findings and determined that URE failed to maintain documentation of all electronic access points to the ESPs and for 60 assets deployed for the access control and monitoring of these access points, in violation of CIP-005-3 R1.6. URE also failed to afford these unidentified access control and monitoring Cyber Assets 27 protective measures, as required by CIP-005-3 R1.5.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the present.

[4] WECC assessed the VRF and VSL for this violation at the requirement level.

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, the risk to the BPS was moderate because URE failed to afford 27 protections to 60 assets associated with access points and access control and monitoring within 100 percent of URE's ESPs. The risk was mitigated by the fact that the Cyber Assets physically reside within the PSP and ESP they were responsible for protecting. Therefore, the Cyber Assets were given physical and electronic monitoring and alarming protection at all time. In addition, URE has a system network that supports systems critical to URE and where traffic is segregated by firewalls. Furthermore, URE's physical access controls restrict access to only approved personnel with approved PRAs and cyber security training.

CIP-005-3 R5

CIP-005-3 R5 provides:

> R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.
>
> > R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.
> >
> > R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
> >
> > R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

CIP-005-3 R5 has a “Lower” VRF and a “Severe” VSL.

During URE's Audit, WECC’s Audit Team reviewed URE's network drawings and configuration manuals and conducted facility site tours to verify URE's assets in the network drawings. During the site tour, the Audit Team identified a discrepancy in a network drawing. Specifically, a network switch was identified on the drawing but was no longer located within the ESP. After discussing the discrepancy with URE, URE stated that the network switch was redeployed to a new ESP.

WECC reviewed the Audit findings and determined that URE was in violation of CIP-005-3 R5.2 for failing to update its documentation to reflect the redeployed CCAs within 90 calendar days of the change.

WECC determined the violation began 90 days after URE failed to update its documentation, and continued through the date 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. Although URE failed to update the ESP network drawing when the asset was removed, the documentation was accurate for URE's remaining ESPs. In addition, all traffic to and from ESPs must pass through firewalls, which are configured to restrict, monitor, and alert upon suspected malicious activity. Further, URE's substation is surrounded by a six-foot-high chain link fence with three-strand barbed wire on top. URE restricts physical access to individuals with PRAs and cyber security training.

CIP-006-1 R1.2 and R1.8

The purpose statement of Reliability Standard CIP-006-1 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 . . . ."

CIP-006-1 R1 provides in pertinent part:

> The Responsible Entity shall comply with the following requirements of Standard CIP-006:
>
> 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:
>
> > R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.
> >
> > ***
> >
> > 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 has a "Medium" VRF and a "Severe" VSL.[5]

During URE's Audit, WECC's Audit Team issued a data request to URE that specified 12 Critical Asset sites the Audit Team would visit. During the course of the site visits, the Audit Team reviewed URE's physical security of CCAs and determined URE failed to identify all access points through each PSP (R1.2) and failed to ensure devices used in the physical access control and monitoring of PSPs were protected per CIP-006-1 R1.8.

WECC's Audit Team identified seven instances at four PSPs where all access points to the PSPs were not documented, as follows:

1. URE failed to identify and document a physical access point through the PSP. The door was secured with a card reader, but had no monitoring measures in place and was not identified on the PSP drawings;

2. URE failed to identify an exit-only access point. The door was locked and secured from outside access by restricted key, and had door contacts that would issue an audible alarm if opened. Additionally, the door was monitored by a camera;

3. URE failed to identify four access points. Specifically, one physical access point (a door) on the first floor and three physical access points (two windows, one roof hatch) on the second floor were not identified. URE believed the door to be sealed, and as such not required to be identified as an access point; and

4. URE failed to identify a physical access point through a PSP. On the south end of the PSP, a roof hatch and two metal plates were installed. All three points of access (roof hatch, two metal plates) had contact alarms installed which would alert upon being opened. The roof hatch was locked from the inside with a dead bolt. The three points of access, which were considered one access point (the equivalent of a double door having two points of access) were not identified or documented as access points to the PSP.

In addition, WECC's Audit Team determined URE was not classifying workstations and control panels capable of granting and revoking access to PSPs as devices used in the access control and monitoring of

[5] WECC assessed the VRF and VSL for this violation at the requirement level.

PSPs. Because URE did not identify these devices as physical access control and monitoring devices, URE could not ensure the devices were provided the protections of CIP-006-1 R1.8.

WECC determined that URE was in violation of CIP-006-1 R1.2 for failing to identify seven PSP access points, and for failing to ensure 118 Cyber Assets used in the access control and monitoring of PSPs were afforded the protections specified in CIP-006-1 R1.8.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE, through the date, 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, the risk to the BPS was moderate because URE failed to afford 27 protections to 118 Cyber Assets, and failed to identify seven access points to four PSPs. However, the risk was mitigated by several factors. The Cyber Assets at issue physically reside within the PSP they were responsible for protecting and were afforded physical and electronic monitoring and alarming at all times. In addition, URE implemented a monitoring solution that would alert URE's personnel if an access point were opened. Furthermore, URE implemented a physical access control that restricts access to personnel with PRAs and cyber security training.

CIP-006-1 R2

CIP-006-1 R2 provides:

> R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> > R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
> >
> > R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
> >
> > R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

> R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

CIP-006-1 R2 has a "Medium" VRF and a "Severe" VSL.

During URE's Audit, WECC's Audit Team identified one access point (two metal plates) next to a fire escape hatch in the ceiling that was not locked. The two metal plates had contact alarms which would alert upon being opened; however, no operational or procedural controls to manage the physical access were implemented. Further, WECC's Audit Team issued a data request to URE, asking URE to describe what physical access protections were applied to the metal coverings. In response, URE confirmed that the two metal coverings, if removed, would generate an alarm. However, there were no additional operational or procedural controls installed to manage physical access.

WECC determined that URE was in violation of CIP-006-1 R2 for failing to document and implement operational and procedural controls to manage physical access at one access point to one substation at all times.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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. Although URE failed to afford operational controls to the access point, if the metal coverings were removed, an alarm would have sounded, alerting URE personnel of the opening. Also, URE's substation at issue was surrounded by a six-foot-high chain link fence with three-strand barbed wire on top. The fence has an intrusion detection system mounted throughout. URE restricted physical access to individuals with PRAs and cyber security training.

CIP-006-1 R3

CIP-006-1 R3 provides:

> 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.

R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

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

During URE's Audit, WECC's Audit Team toured one of URE's substations. During the tour, the Audit Team discovered one access point (a door) located on the northwest side of the substation that was not identified on the PSP map provided by URE. The door had no exterior hardware providing for ingress to the PSP and had no means of monitoring in the event the door was open (forced or propped). WECC's Audit Team also toured URE's another transmission operator control PSP. During this site tour, the auditors discovered three access points (doors) which did not have door contacts installed. Therefore, the access points could not be monitored for door-forced-open or door-held-open events.

WECC determined that URE was in violation of CIP-006-1 R3 for failing to implement technical controls for monitoring physical access at all times at four access points (doors) to two PSPs.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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, URE failed to monitor physical access at four access points to two PSPs for approximately four years. Because URE failed to implement these controls, URE could not determine if one of the unmonitored access points were left propped open, thereby allowing unauthorized access to the 72 CCAs located in one PSP and 31 CCAs located at another PSP. However, the risk was mitigated by several factors. The access point at issue was egress only with no external hardware. Also, the substation was surrounded by a six-foot-high, chain link fence with three-strand barbed wire on top and an intrusion detection system mounted throughout. The fence restricted physical access to individuals with PRAs and cyber security training. The other PSP access points had ingress card readers installed, which had to be used to gain access to the locked doors. URE employs security guards, stationed on the ground floor, who verify all personnel that enters the building and validate personnel's access cards.

CIP-007-1 R1

The purpose statement of Reliability Standard CIP-007-1 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 . . . ."

CIP-007-1 R1 provides:

> The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):
>
> R1. 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, 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 cybersecurity 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-007-1 R1 has a "Medium" VRF and a "Severe" VSL.

During URE's Audit, WECC's Audit Team determined URE was not able to produce records of testing for all significant changes to Cyber Assets within an ESP. Specifically, URE could not produce records for three significant changes made to an asset area and four significant changes made to another asset area. In addition, the Audit Team confirmed that URE only performs functional testing and does not perform security testing as part of its test procedures.

WECC determined that URE did not provide any evidence of security testing performance for seven significant changes made to Cyber Assets in the two asset area ESPs. Because URE did not perform

security testing on these seven assets, URE could not ensure that these changes did not adversely affect existing cyber security controls.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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, URE failed to perform security testing on seven assets and could not ensure systems were secure prior to the implementation of software upgrades, vendor releases, version upgrades, and system upgrades. However, the risk was mitigated by several factors. URE had layers of security controls in place during the pendency of the violation. Specifically, URE had network separation with firewall technology, host intrusion detection systems, annual cyber vulnerability assessments, and monitoring and alerting processes that included third-party analysis and reporting. Additionally, all traffic to and from URE's ESPs passed through multiple firewalls, which were configured to restrict, monitor, and alert upon suspected malicious activity. Lastly, URE performs functionality testing on all assets prior to making significant changes. This type of testing verifies that the device operates correctly prior to being released into production.

CIP-007-1 R2

CIP-007-1 R2 provides:

> R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> > R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
> >
> > R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
> >
> > R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R2 has a “Medium” VRF and a “Severe” VSL.

During URE's Audit, WECC's Audit Team identified eight power supply controllers that had ports open and were not required for normal or emergency operations, but could not be disabled. The ports were used for remote logging and for securing systems determined to be CCAs.

WECC determined URE was in violation of CIP-007-1 R2 for failing to enable only those ports and services required for normal and emergency operations. WECC also determined that URE failed to document compensating controls and submit a Technical Feasibility Exception (TFE) for the eight devices that had ports open that were not required but could not be disabled.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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, URE failed to document compensating controls and submit a TFE for the eight RAS devices that have ports open that are not required but could not be disabled. The ports were used for remote logging and for securing systems determined to be CCAs. However, the risk was mitigated by several factors. URE used network and host intrusion detection and protection systems to provide protection against attacks, exploits, and vulnerabilities. This system included network separation and firewall technology which was monitored at all times. URE's devices were physically secure because URE used ID badge systems, cameras, and physical security monitors to deter and prevent unauthorized physical access to areas or systems. Further, all individuals with access to ESPs and PSPs had PRAs and cyber security training.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of four hundred sixty-five thousand dollars ($465,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. URE's prior violation history for CIP-006-1 R1, which was not considered an aggravating factor in the penalty determination;[6]
2. URE's prior violation history for CIP-007-1 R2, which was considered an aggravating factor in the penalty determination;[7]

[6] Although this was URE's third violation of CIP-006-1 R1, WECC determined the first and second instances are distinct from this violation because they relate to separate sub-requirements. As a result, WECC determined that this was not recurring conduct and aggravation was not warranted for the violation addressed herein.

[7] This was URE's second violation of CIP-007-1 R2. Similar to the instant violation, the first violation involved URE's failure to establish and document a process to ensure that only those ports and services required for normal and emergency

3. URE's prior violation history for CIP-007-1 R1 was not considered as an aggravating factor by WECC;[8]
4. URE had a compliance program at the time of the violation which WECC considered a mitigating factor;
5. URE was cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
8. 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 four hundred sixty-five thousand dollars ($465,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[9]

CIP-002-2 R3

URE's Mitigation Plan to address its violation of CIP-002-2 R3 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. update its RBAM to clarify timelines and requirements;
2. develop a procedure for semi-annual sampling and verification of the CCA list;
3. create a process map for management of relevant changes that can be used by all stakeholders;
4. select a common database for CCAs;
5. establish and complete semi-annual CCA audit; and

operations were enabled for approximately 400 devices. Therefore, WECC considered the previous violation as an aggravating factor in the penalty determination.

[8] This was URE's fourth violation of CIP-007-1 R1. Because the prior violations were concurrent with the instant violation, WECC did not consider them as an aggravating factor in the penalty determination.

[9] *See* 18 C.F.R § 39.7(d)(7).

6. review the status of the audit and make appropriate updates.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-3 R1

URE's Mitigation Plan to address its violation of CIP-005-3 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. perform a detailed analysis and extent of condition of the entire CIP-related environment to determine whether existing documentation needs to be updated or clarified, and whether additional systems or assets need to be included;
2. finalize the implementation plan to ensure ongoing compliance with CIP-005 R1;
3. create a detailed scope of work and project plan based on the completed extent of condition review;
4. create documentation and processes required to support completion of the project;
5. develop training materials needed to ensure all stakeholders are trained as required on the changes being implemented into the CIP environment;
6. complete implementation of the updated processes; and
7. complete training for all key stakeholders as required.

CIP-005-3 R5

URE's Mitigation Plan to address its violation of CIP-005-3 R5 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform an extent of condition review to ensure URE fully understands the overall scope of the finding and include all relevant assets and areas in the remediation activities;
2. create a process and procedure for performing annual site visits and walk-downs of ESPs;
3. implement the site visit and walk-down procedure;
4. create a formalized, documented process that will ensure that drawings and associated documentation is consistently managed in compliance with the requirements of CIP-005 R5;

5. develop training related to the new process for key stakeholders; and
6. implement the new process and training.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-1 R1

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 was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. provide site contacts with special locks and instructions in order to control access at identified sites;
2. have the applicable stakeholders meet quarterly to review Critical Asset ESP and PSPs;
3. identify resources and draft a timeline to remove assets out of ESPs;
4. update the Cyber Asset list with additional fields and include a change tab to document all changes;
5. move the assets at issue out of the ESP;
6. document a communication process to notify key stakeholders when an asset is added to existing ESPs; and
7. update documentation to reflect change at the locations at issue.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-1 R2

URE's Mitigation Plan to address its violation of CIP-006-1 R2 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. review the CIP-006-3 R4 (CIP-006-1 R2) requirement regarding the definition of access point with the manager, supervisor, security vendor and physical security specialists;
2. instruct the security vendor to eliminate the roof hatch from being an access point;
3. reconfigure the PSP and install card readers and door contacts on the interior door that controls access to the PSP;

4. update the diagram for a substation when changes are made to the PSP; and
5. implement a quarterly PSP review process to review PSP diagrams for accuracy.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-1 R3

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 was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. hire additional resources to conduct PSP site visits and review diagrams for accuracy;
2. install the missing door contacts to two facilities, and update the diagrams;
3. implement quarterly PSP review processes which include reviewing physical access controls at PSPs; and
4. update PSP diagrams to a standard format.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R1

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform an extent of condition review to identify the gaps in the process and establish what assets areas are impacted;
2. create a plan (scope of work) with additional, specific milestones and identify key stakeholders and roles and responsibilities associated with the work to be completed. The plan includes standardized test criteria and test plans, cyber security controls checklist, quality assurance processes, and description of maintaining and storing evidence. The plan also includes integration into existing change management procedures, as appropriate;
3. create a training plan to be delivered to key stakeholders involved in the security controls testing process;
4. complete implementation of the modified test procedures;
5. update documentation and associated information as appropriate;

6. complete training of key stakeholders; and
7. implement effective controls to ensure ongoing compliance.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R2

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. complete a targeted port scan of the power supply controllers to determine a complete list of all of the open ports;
2. review all vendor ports and services documentation;
3. update the list to reflect ports and submit a TFE;
4. perform an extent of condition review to ensure the overall scope is clearly defined and understood;
5. evaluate the other devices to confirm the accuracy of the list, and determine whether any additional TFEs are required; and
8. update URE's list and complete and submit TFEs if required.

URE certified on that the above Mitigation Plan requirements were completed. After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[10]

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,[11] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on November 5,

[10] *See* 18 C.F.R. § 39.7(d)(4).
[11] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

2013. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a four hundred sixty-five thousand dollar ($465,000) 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. URE's prior violations for CIP-006-1 R1, CIP-007-1 R1 and R2, as discussed above;
2. URE had a compliance program at the time of the violations which WECC considered a mitigating factor, as discussed above;
3. WECC reported that URE was cooperative throughout the compliance enforcement process;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
6. 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 four hundred sixty-five thousand dollars ($465,000) 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.

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the attached documents are deemed confidential by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

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) 713-9598
(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) 883-6885
(801) 883-6894 – facsimile
CWhite@wecc.biz

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

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.	

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

cc: URE
Western Electricity Coordinating Council

Attachments