PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

July 31, 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. NP13-_-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 the 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-004-1 R4; CIP-005-1 R1 and R2; CIP-005-3 R3; CIP-006-1 R1; and CIP-007-1 R2, R3, R4, R5, and R6. 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 ninety-eight thousand dollars ($198,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance

[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 (2011). *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.

under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC2011008651; WECC2011008652; WECC2011008653; WECC2011008654; WECC2012011489; WECC2011008657; WECC2011008658; WECC2011008659; WECC2011008660; and WECC2011008661 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 May 31, 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-2055	WECC2011008651	CIP-004-1	R4	Lower	$198,000
			WECC2011008652	CIP-005-1	R1	Medium	
			WECC2011008653	CIP-005-1	R2	Medium	
			WECC2011008654	CIP-005-3	R3	Medium	
			WECC2012011489	CIP-006-1	R1	Medium	
			WECC2011008657	CIP-007-1	R2	Medium	
			WECC2011008658	CIP-007-1	R3	Lower	

			WECC2011008659	CIP-007-1	R4	Medium	
			WECC2011008660	CIP-007-1	R5	Medium	
			WECC2011008661	CIP-007-1	R6	Lower[4]	

CIP-004-1 R4

The purpose statement of Reliability Standard CIP-004-1 provides in pertinent part:

> Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-004-1 R4 provides:

> R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
>
> > R4.1. The Responsible Entity[5] shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

[4] The Settlement Agreement incorrectly states that the VRF for this violation is Medium.

[5] Within the text of the Standards included in this Full Notice of Penalty, "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.

> R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-004-1 R4 has a "Lower" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE submitted a Self-Report citing noncompliance with CIP-004-1 R4. In its Self-Report, URE disclosed that users with certain shared system accounts were not listed as having access to Critical Cyber Assets (CCAs). WECC subject matter experts (SMEs) reviewed URE's Self-Report and determined that 40 individuals with access to 28 shared accounts were not listed as having electronic access to CCAs.

WECC Enforcement reviewed URE's Self-Report, SMEs' findings, and additional information submitted by URE. For approximately four months, URE disclosed that the scope of the CIP-004-1 R4 violation was greater than that initially disclosed in its Self-Report. URE reported that it failed to update access lists for 6 individuals; it failed to conduct quarterly reviews for 80 individuals; and it incorrectly identified 2 individuals as having access to CCAs. Further, URE reported that it failed to identify individuals with access to 55 shared accounts and 60 individual accounts that provisioned electronic access to CCAs.

In total, URE reported that it failed to list individuals with access to 60 individual accounts and a total of 55 shared accounts. In response to WECC Enforcement's requests, URE could not identify specific individuals who maintained electronic access to CCAs using these shared accounts.

The CCAs to which individuals had access included remote terminal units (RTUs), database servers, Ranger applications (energy management systems (EMSs)), domain controllers, file servers, and virtual desktops used to control supervisory control and data acquisition (SCADA).

WECC Enforcement, therefore, determined that URE failed to identify and list individuals with electronic access to CCAs and failed to maintain access lists in violation of CIP-004-1 R4.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through when 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 was mitigated by the following factors. URE staff with access to individual accounts all completed personnel risk assessments (PRAs) and cybersecurity training. The CCAs in scope of the violation were physically and electronically protected. The CCAs were physically secured within Physical Security Perimeters (PSPs). All physical access was logged and monitored, and any unauthorized physical access attempts would have triggered alarming. The CCAs in scope of the violation were also afforded a number of electronic protections that mitigated the risk during the pendency of the violation. All CCAs were located within an Electronic Security Perimeter (ESP). Electronic access was logged and monitored, and any cybersecurity events within ESPs would have triggered alarming. Further, all individuals with access to accounts would have had to use a password to access any CCA electronically.

CIP-005-1 R1

The purpose statement of Reliability Standard CIP-005-1 provides: "Standard CIP-005 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 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-005-1 R1 provides:

> The Responsible Entity shall comply with the following requirements of Standard CIP-005:
>
> > 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).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP- 003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

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-005-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report citing noncompliance with CIP-005-1 R1. Specifically, URE reported that it was discovered that an access point to an ESP was not properly identified and documented. WECC SMEs reviewed URE's Self-Report and contacted URE requesting additional information. The SMEs determined that URE failed to identify a total of nine ESP access points and that the nine devices were externally connected with an end point terminating at a device within the ESP. The SMEs determined that the devices were access points to an ESP containing 339 CCAs associated with two of URE's control centers. WECC SMEs found URE in violation of CIP-005-1 R1 and forwarded their findings to WECC Enforcement.

WECC Enforcement reviewed URE's Self-Report and SMEs' findings and determined that the nine devices were access points to an ESP associated with URE's control center. Further, WECC Enforcement determined that URE's failure to identify and document the devices as ESP access points constitutes a violation of CIP-005-1 R1.1. In addition to being access points, the devices in scope also provision access control and monitoring to the ESP.

WECC Enforcement issued URE a Notice of Alleged Violation (NOAV) of CIP-005-1 R1. Approximately a month later, URE submitted its NOAV response in which URE requested to enter settlement negotiations. After URE submitted its NOAV response, the scope of the violation expanded. For approximately four months 2, the scope of URE noncompliance expanded to include a total of 127 devices.

WECC Enforcement determined that URE failed to afford all the protective measures described under CIP-005-1 R1.5 to an additional 118 devices not included in the NOAV or in URE's original Mitigation Plan. WECC Enforcement, therefore, determined that the full scope of URE noncompliance included the following:

1. URE failed to identify and document nine ESP access points that were also used as Cyber Assets in the ESP, in violation of R1.1, R1.5 and R1.6; and

2. URE failed to afford all protective measures described in R1.5 to additional 118 Cyber Assets used in the ESP.

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

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's failure to identify and secure the ESP access points exposed 339 CCAs associated with two control centers to cyber attack or misuse. However, the risk was mitigated by the following factors. The nine ESP access points and associated devices were physically secured within a PSP. The individuals with physical access to the devices had completed PRAs and CIP cybersecurity training required under CIP-004-1.

CIP-005-1 R2

CIP-005-1 R2 provides:

> Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
>
> R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

CIP-005-1 R2 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report for a violation with CIP-005-1 R2. Specifically, URE reported that it failed to implement mechanisms that deny electronic access by default, in violation of CIP-005-1 R2.1. Further, URE reported that it failed to ensure that only ports and services required for normal and emergency operations were enabled, in violation of R2.2. URE also reported a violation of R2.4 because it failed to implement strong controls that ensured authentication on four hosts with external access into an ESP.

WECC SMEs reviewed URE's Self-Report and contacted URE on three separate occasions to request additional information and clarification.

The SMEs determined that the violation of CIP-005-1 R2 was threefold. First, SMEs determined that four corporate servers allowed access through the ESP boundary without triggering any authentication control at the ESP boundary in violation of R2.1. Second, URE failed to ensure that only ports and services required for normal and

emergency operations were enabled pursuant to R2.2. Lastly, SMEs determined that nine servers enabled external access to the ESP without requiring two-factor identification.

WECC Enforcement reviewed URE's Self-Report and SMEs' findings and determined that URE failed to implement mechanisms to control and secure electronic access at 13 ESP access points in violation of CIP-005-1 R2.1, R2.2, and R2.4.

After WECC issued a NOAV, URE disclosed additional instances of noncompliance that expanded that scope of the CIP-005-1 R2 violation. URE reported that it failed to implement strong procedural or technical controls to ensure authenticity of accessing party at 10 additional access points and one Citrix device in violation of R2.4. The scope of this violation includes a total of 23 access points.

WECC Enforcement determined that URE failed to implement access controls as required under CIP-005-1 R2 at 23 access points.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The devices in scope of the violation were associated with URE's control systems. Unauthorized access gained through any one of the four corporate servers would not have been logged, monitored, or tracked. WECC did, however, consider URE's compensating measures in place during the violation period. Specifically, the 13 access points were located in a physically secure facility with video monitoring and card key restrictions. The devices that could gain access to the ESP without two-factor authentication were located in the corporate environment that required appropriate credentials to gain access. URE implemented an intrusion detection system that was actively monitoring the ESP and was configured for automatic alerting.

CIP-005-3 R3

CIP-005-3 R3 provides:

> R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for

monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

CIP-005-3 R3 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report citing noncompliance with CIP-005-3 R3. Specifically, URE reported that it disabled logging and monitoring at an ESP access point for approximately forty days.

WECC SMEs reviewed URE's Self-Report and the SMEs contacted URE requesting additional information. Based on the information disclosed by URE, SMEs determined that URE took its power plant offline and powered down its secure dial-up gateway ESP access point. A single management port on the secure dial-up access control device, however, remained connected to the internet and continued to provision dial-up access to CCAs and Cyber Assets within the ESP. Because devices provisioning ESP monitoring and logging were also powered down, dial-up access through the active management port was neither logged nor monitored.

WECC Enforcement determined that the violation was from the date URE's devices provisioning ESP monitoring and logging were also powered down through when the violation was discovered and the port was disabled.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, the risk was mitigated by the following factors.

The CCAs within the ESP were located in a PSP and were afforded the protections of CIP-006. Additionally, while the secure dial-up access control device was powered down, the facility associated with these CCAs and Cyber Assets, was also powered down during the violation period for maintenance and testing. Therefore, the potential for malicious activity during the period of maintenance was reduced.

CIP-006-1 R1

The purpose statement of Reliability Standard CIP-006-1 provides: "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:
> >
> > > R1.1. 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.

CIP-006-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report citing noncompliance with CIP-006-1 R1. In its Self-Report, URE stated that during the course of an internal Compliance Audit, URE discovered eight PSPs located in two facilities that were not constructed to ensure six-walled protection as required under CIP-006-1 R1.1. URE reported that it discovered gaps greater than 96 square inches in the wire mesh used to construct seven of the PSPs. Further, URE

reported that three out of four corners of a wire mesh wall comprising another PSP ceiling were left unsecured.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for 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. Specifically, the risk was mitigated by the following factors. URE deployed a layered approach to physical security. All PSPs were housed in buildings that had restricted and monitored physical access. All access to these facilities was logged. Authorized access was limited to individuals who required such access, and who had completed PRAs and cybersecurity training. Unauthorized access attempts would have triggered alerts to URE security personnel. Further, ingress and egress at all PSP access points was monitored on a 24-hour, seven days a week basis by onsite security personnel. CCAs within the PSPs required authentication. Unauthorized log-in access attempts would have triggered alarming. Although one "wall" of each of the eight PSPs was not secured, unsecured wire mesh comprised the "ceiling" of the PSPs. The mesh was installed behind ceiling tiles and was not readily accessible.

CIP-007-1 R2

The purpose statement of Reliability Standard CIP-007-1 provides:

> 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 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.

URE submitted a Self-Report citing noncompliance with CIP-007-1 R2. Specifically, URE reported that it failed to ensure that only those ports and services required for normal and emergency operations were enabled.

WECC SMEs reviewed URE's Self-Report and contacted the entity to request additional information. WECC's SMEs determined that the scope of the Self-Report included 48 CCAs and 61 non-critical Cyber Assets within an ESP associated with URE's control center and backup control center. WECC SMEs determined that URE failed to ensure that only ports and services required for normal and emergency operations were enabled on these devices.

URE relied exclusively on vendor documentation, and did not conduct independent assessments of ports and services required for normal and emergency operations in the context of URE's system.

WECC determined the duration of the violation to be the date the Standard became mandatory and enforceable for 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. The 109 devices in scope of the violation are associated with URE control centers. URE's failure to secure ports and services on these devices exposes multiple ESPs to cyber attack or misuse. However, the risk was mitigated by the following factors. All CCAs and Cyber Assets within ESPs were physically secured within a PSP. Individuals with physical and electronic access to these devices completed PRAs and cybersecurity training. All electronic access was controlled, logged, and monitored.

CIP-007-1 R3

CIP-007-1 R3 provides:

> R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
>
> > R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
> >
> > R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R3 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report citing noncompliance with CIP-007-1 R3. Specifically, URE reported that it failed to assess security patches within 30 days of being made available for 76 devices in its operating system environment, visualization software, and ancillary systems.

WECC Enforcement issued a NOAV and after the NOAV was issued, URE disclosed that the scope of the violation had expanded to include 132 devices in total.
WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for 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, the devices at issue were associated with URE's control centers. However, the risk was mitigated by the following factors. URE logged and monitored electronic and physical access to the CCAs and

Cyber Assets in scope. Individuals with physical and electronic access to these devices completed PRAs and cybersecurity training.

CIP-007-1 R4

CIP-007-1 R4 provides:

> R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
>
> R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.
>
> R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

CIP-007-1 R4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report citing noncompliance with CIP-007-1 R4. Specifically, URE reported that it failed to use antivirus software or malware prevention tools on some Cyber Assets within the ESP but did not identify the number of assets at issue.

WECC SMEs contacted URE and requested additional information. Based on the provided information, the SMEs determined that URE failed to implement antivirus software and malware prevention tools on 46 of its non-Windows based Cyber Assets.

WECC sent a NOAV to URE. After the NOAV was issued, URE disclosed that the scope of the violation expanded and URE failed to implement antivirus software on 192 devices in total. Further, URE disclosed that it failed to file Technical Feasibility Exceptions (TFEs) for the 192 devices in a timely manner.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for 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, URE's control center systems were exposed to malicious attack or misuse for a period of almost three years. WECC did, however, consider URE's compensating measures in place during the violation period. All devices were located within a PSP. Individuals with physical and logical access to devices had completed PRAs and cybersecurity training. All devices were located within an ESP within electronic access that was controlled and monitored.

CIP-007-1 R5

CIP-007-1 R5 provides:

> 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.
>
> > R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
> >
> > > R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.
> >
> > > R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.
> >
> > > R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in

accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

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.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

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

R5.3.1. Each password shall be a minimum of six characters.

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

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

CIP-007-1 R5 has a “Medium” VRF and a “Severe” VSL.

URE submitted a Self-Report citing noncompliance with CIP-007-1 R5. Specifically, URE reported that some shared accounts on some devices had not been previously identified and, therefore, were not afforded the protections prescribed under CIP-007-1 R5. URE did not identify the number of devices at issue.

WECC Enforcement determined that the scope of the violation indicated URE failed to identify a total of 60 individual accounts and 94 shared accounts, provisioning access to 180 devices.

WECC Enforcement determined the duration of the violation to be from the date the Standard became mandatory and enforceable for 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, the risk was mitigated by the following factors. All devices were secured within URE's PSP and ESP. Electronic and physical access was controlled, monitored, and logged. Shared account use was also logged and monitored. All users completed PRAs and cybersecurity training.

CIP-007-1 R6

CIP-007-1 R6 provides:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> > R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
> >
> > R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-1 R6 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report citing noncompliance with CIP-007-1 R6. URE reported that it failed to implement automated tools or organizational processes to control and monitor system events related to cybersecurity on 339 devices within one ESP. WECC determined that the devices were either not configured, configured incorrectly, or not capable of logging and monitoring.

WECC Enforcement reviewed URE's Self-Report and WECC SMEs' findings and determined that URE failed to implement technical and procedural mechanisms for monitoring cybersecurity events on the Cyber Assets within the ESP.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through when WECC 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 was mitigated by the following factors. All devices were contained within a PSP with restricted and logged physical access. The devices were also within an ESP and behind firewalls that restricted and logged logical access into the ESP. Individuals with access to these devices had completed PRAs and cybersecurity training.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred ninety eight thousand dollars ($198,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. URE had an internal compliance program (ICP) during the pendency of the violations, which was considered a mitigating factor in the penalty determination;
2. WECC Enforcement considered URE's violation history but determined that it should not serve as an aggravating factor in the penalty determination;
3. URE self-reported the violations;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violations 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.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred ninety-eight thousand dollars ($198,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[6]

CIP-004-1 R1

URE's Mitigation Plan to address its violation of CIP-004-1 R1 was submitted to WECC as complete. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007304 and was submitted as non-public information to FERC in accordance with FERC orders.

[6] *See* 18 C.F.R § 39.7(d)(7).

URE's Mitigation Plan required URE to:

1. Identify and document all shared accounts at critical facilities and include all related access user lists in its established CIP-004 access management processes;
2. Complete remediation of identified and undocumented shared accounts at a control center;
3. Complete extended review for unidentified shared accounts at URE's control center and generation;
4. Obtain stakeholder approval of its plan to address remediation items that are required to address the deficiencies associated with this violation;
5. Perform mid-course verification to ensure remediation items are on track according to the Mitigation Plan; and
6. Develop refresher training for relevant personnel.

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

After reviewing URE's submitted evidence, WECC accepted URE's Certification of Mitigation Plan Completion.

CIP-005-1 R1

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was submitted as complete to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT006650 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Identify the hosts to be moved to the demilitarized zone (DMZ) or retired;
2. Modify firewall rules to deny the cryptographic network protocol. Data that was required by the connection was moved to the DMZ at which point the process picks up the data, as opposed to directly from the DMZ;
3. Review other URE ESPs;
4. Remediate items discovered through extended review process;
5. Complete extended review of other existing URE ESPs;

6. Develop and obtain stakeholder approval of plan to address remediation items required to address deficiencies as part of extended review;
7. Perform mid-course verification to ensure remediation items are on track; and
8. Complete data collection.

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

After reviewing URE's submitted evidence, WECC rejected the Certification of Completion because additional assets needed to be added to the Mitigation Plan, and directed URE to submit a revised Mitigation Plan.[7]

CIP-005-1 R2

URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT006651-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Complete remediation of the identified issues within the ESP environment;
2. Gather data required to perform review of other existing URE ESP access points;
3. Complete assessment of findings and obtain stakeholder approval of its plan to address the assessment findings;
4. Perform mid-course verification to ensure that remediation is on track; and
5. Complete remediation of the issues.

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

[7] As of July 29, 2013, WECC has notified NERC that URE has not yet submitted the revised Mitigation Plan.

After reviewing URE's submitted evidence, WECC rejected the Certification of Completion because additional assets needed to be added to the Mitigation Plan, and directed URE to submit a revised Mitigation Plan.[8]

CIP-005-3 R3

URE's Mitigation Plan to address its violation of CIP-005-3 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 WECCMIT006653 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Physically remove the secure dial-up access control device units from URE's plant devices and network;
2. Complete and verify the completion of the decommissioning process; and
3. Gather required compliance documentation.

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

After reviewing URE's submitted evidence, WECC accepted URE's Certification of Mitigation Plan Completion.

CIP-006-1 R1

URE's Mitigation Plan to address its violation of CIP-006-1 was submitted to WECC on. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT008689 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Complete inspection of all PSPs;
2. Complete reconstruction of the eight PSPs identified as being deficient; and
3. Ensure that project managers oversee completion of PSP construction.

[8] As of July 29, 2013, WECC has notified NERC that URE has not yet submitted the revised Mitigation Plan.

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

After reviewing URE's submitted evidence, WECC accepted URE's Certification of Mitigation Plan Completion.

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 is designated as WECCMIT006652 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Complete remediation of the issues identified within the ESP environment;
2. Complete extended review of other existing URE ESPs;
3. Obtain stakeholder approval of plan to address remediation of items required to resolve any compliance deficiencies;
4. Complete any identified remediation items; and
5. Gather required compliance documentation.

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

After reviewing URE's submitted evidence, WECC accepted URE's Certification of Mitigation Plan Completion.

CIP-007-1 R3

URE's Mitigation Plan to address its violation of CIP-007-1 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 WECCMIT006654 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Complete remediation of the issues identified within the ESP environment;
2. Complete extended review of other existing URE ESPs;

3. Obtain stakeholder approval of plan to address remediation of items required to resolve any compliance deficiencies;
4. Complete any identified remediation items; and
5. Gather required compliance documentation.

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

After reviewing URE's submitted evidence, WECC accepted URE's Certification of Mitigation Plan Completion.

CIP-007-1 R4

URE's Mitigation Plan to address its violation of CIP-007-1 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 WECCMIT006655 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Complete remediation of the issues identified within the ESP environment;
2. Complete extended review of other existing URE ESPs;
3. Obtain stakeholder approval of plan to address remediation of items required to resolve any compliance deficiencies;
4. Complete any identified remediation items; and
5. Gather required compliance documentation.

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

After reviewing URE's submitted evidence, WECC accepted URE's Certification of Mitigation Plan Completion.

CIP-007-1 R5

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted as complete to WECC. The Mitigation Plan was accepted by WECC and approved by NERC.

The Mitigation Plan for this violation is designated as WECCMIT006656 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Complete remediation of the issues identified within the ESP environment;
2. Complete extended review of other existing URE ESPs;
3. Obtain stakeholder approval of plan to address remediation of items required to resolve any compliance deficiencies;
4. Complete any identified remediation items; and
5. Gather required compliance documentation.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted a document showing that the milestone activities were completed and refresher training was developed.

As of the date of the filing, WECC has not finished verifying completion of the Mitigation Plan for this violation.

CIP-007-1 R6

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT006657 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Complete remediation of the issues identified within the ESP environment;
2. Complete extended review of other existing URE ESPs;
3. Obtain stakeholder approval of plan to address remediation of items required to resolve any compliance deficiencies;
4. Complete any identified remediation items; and
5. Gather required compliance documentation.

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

After reviewing URE's submitted evidence, WECC accepted URE's Certification of Mitigation Plan Completion.

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 NERC BOTCC reviewed the Settlement Agreement and supporting documentation on July 9, 2013. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred ninety-eight thousand dollars ($198,000) 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 had a compliance program at the time of the violation which WECC considered a mitigating factor, as discussed above;
2. URE's history of noncompliance was a neutral factor in the penalty determination;
3. URE self-reported the violations;
4. WECC reported that URE was cooperative throughout the compliance enforcement process;

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

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 ninety-eight thousand dollars ($198,000) 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.

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

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

a) Settlement Agreement by and between WECC and URE, included as Attachment a;

b) Record documents for the violation of CIP-004-1 R4, included as Attachment b:

   1. URE's Self-Report for CIP-004-1 R4;
   2. URE's Mitigation Plan designated as WECCMIT007304;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Notice of Completed Mitigation Plan Acceptance;

c) Record documents for the violation of CIP-005-1 R1, included as Attachment c:

   1. URE's Self-Report for CIP-005-1 R1;
   2. URE's Mitigation Plan designated as WECCMIT006650;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Notice of Completed Mitigation Plan Rejection and Request for Revised Mitigation Plan;

d) Record documents for the violation of CIP-005-1 R2, included as Attachment d:

   1. URE's Self-Report for CIP-005-1 R2;
   2. URE's Mitigation Plan designated as WECCMIT006651-2;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Notice of Completed Mitigation Plan Rejection and Request for Revised Mitigation Plan;

e) Record documents for the violation of CIP-005-3 R3, included as Attachment e:

   1. URE's Self-Report for CIP-005-3 R3;
   2. URE's Mitigation Plan designated as WECCMIT006653;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Notice of Completed Mitigation Plan Acceptance;

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

1. URE's Self-Report for CIP-006-1 R1;
2. URE's Mitigation Plan designated as WECCMIT008689;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Notice of Completed Mitigation Plan Acceptance;

g) Record documents for the violation of CIP-007-1 R2, included as Attachment g:

1. URE's Self-Report for CIP-007-1 R2;
2. URE's Mitigation Plan designated as WECCMIT006652;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Notice of Completed Mitigation Plan Acceptance;

h) Record documents for the violation of CIP-007-1 R3, included as Attachment h:

1. URE's Self-Report for CIP-007-1 R3;
2. URE's Mitigation Plan designated as WECCMIT006654;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Notice of Completed Mitigation Plan Acceptance;

i) Record documents for the violation of CIP-007-1 R4, included as Attachment i:

1. URE's Self-Report for CIP-007-1 R4;
2. URE's Mitigation Plan designated as WECCMIT006655;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Notice of Completed Mitigation Plan Acceptance;

j) Record documents for the violation of CIP-007-1 R5, included as Attachment j:

1. URE's Self-Report for CIP-007-1 R5;
2. URE's Mitigation Plan designated as WECCMIT006656;
3. URE's Certification of Mitigation Plan Completion;

k) Record documents for the violation of CIP-007-1 R6, included as Attachment k:

1. URE's Self-Report for CIP-007-1 R6;
2. URE's Mitigation Plan designated as WECCMIT006657;

3. URE's Certification of Mitigation Plan Completion; and
4. WECC's Notice of Completed Mitigation Plan Acceptance.

A Form of Notice Suitable for Publication[11]

A copy of a notice suitable for publication is included in Attachment l.

[11] *See* 18 C.F.R § 39.7(d)(6).

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) 883-6855 (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 Christopher 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