PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

January 30, 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, 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-006 and CIP-007. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred nine thousand dollars ($109,000), 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 WECC201102978, WECC2012010727, WECC2012010728, WECC2012010729, and WECC2012010730 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

---

[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.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on December 16, 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-2263	WECC201102978	CIP-006-1	R1	Medium	$109,000
			WECC2012010727	CIP-006-3a	R5	Medium	
			WECC2012010728	CIP-007-1	R2	Medium	
			WECC2012010729	CIP-007-1	R3	Lower	
			WECC2012010730	CIP-007-1	R6	Medium	

CIP-006

The purpose statement of Reliability Standard CIP-006 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

CIP-006-1 R1 provides:

> R1. Physical Security Plan — The Responsible Entity[4] shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
> >
> > R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.
> >
> > R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).
> >
> > R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
> >
> > R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.
> >
> > R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.
> >
> > R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

[4] Within the text of Standards CIP-002 through CIP-009, "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.

> R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.
>
> R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

[Footnote added.]

CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5, and R1.6 each have a "Medium" VRF and a "Severe" Violation Severity Level (VSL). CIP-006-1 R1.7, R1.8, and R1.9 each have a "Lower" VRF.

URE submitted a Self-Certification to WECC addressing noncompliance with CIP-006-1 R1. Specifically, URE reported that during an on-site assessment conducted by an external vendor, the vendor observed that there was an openly accessible human machine interface (HMI), classified as a Critical Cyber Asset (CCA), on the exterior wall of a Physical Security Perimeter (PSP). The HMI is a touch screen monitor allowing for local control of equipment. These HMIs communicate with programmable logic controllers (PLCs). Upon further examination, URE identified that this situation also existed at three other identically designed facilities. WECC determined that URE failed to provide a completely enclosed six-wall border to eight CCAs.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE removed the HMI monitors from service.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). The CCAs had 24 hour a day, seven day a week physical and electronic monitoring and alarming. URE's control rooms are manned continuously and the control room operator monitor alerts regarding any unexpected activity at the HMIs. In the event that an HMI is compromised, alarms immediately notify personnel responsible for response. In addition, the devices have a restrictive operating system that limits physical access at the face of the devices.

CIP-006-3a R5
CIP-006-3a R5 provides:

> R5. 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-008-3. One or more of the following monitoring methods shall be used:
>
> • 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.
>
> • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

CIP-006-3a R5 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Certification to WECC addressing noncompliance with CIP-006-3c R5. Specifically, URE reported six incidents where it failed to implement its technical and procedural controls for monitoring physical access at access points to the PSPs 24 hours a day, seven days a week:

1. For approximately two hours, URE's physical access control and monitoring (PACM) server failed and was not actively monitoring logs sent from the physical access points to six PSPs;
2. For approximately one hour, URE's PACM server failed and was not actively monitoring logs sent from the physical access points to six of its PSPs;
3. For approximately ten minutes, URE's PACM server failed and was not actively monitoring logs sent from the physical access points to six of its PSPs;
4. For approximately four hours, URE's PACM server failed and was not actively monitoring logs sent from the physical access points to four of its PSPs;
5. For approximately two hours, URE's PACM server failed and was not actively monitoring logs sent from the physical access points to four of its PSPs; and
6. A URE system operator disarmed a PSP's two access points but failed to re-arm the access points when finished, resulting in a failure to provide access monitoring for 17 hours.

WECC determined the duration of the violation to be from the date on which URE first failed to implement the controls for monitoring access at all access points to the PSPs, 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, failure to monitor physical access at all access points to the PSPs could allow unauthorized access to the PSP to go unnoticed and unchecked, potentially allowing malicious access to Cyber Assets. Individuals could then use such access to cause harm to CCAs essential to the operation of the BPS.

The five instances where the PACM server failed were unplanned, and ranged from ten minutes to four hours. This reduced the likelihood that a malicious actor would know of the outages and have the opportunity to gain malicious access to Cyber Assets. For the sixth instance, the PSP resided in a secure facility where physical access is monitored and restricted by use of a card key. Therefore, even though the specific cabinet and CCA were not re-armed, there were still only a select few individuals with access to the room where the cabinet was housed, and the CCA required appropriate credentials to gain access. Accordingly, even though the drawer was unlocked and unarmed, a malicious actor would require appropriate logical credentials to access the drawer.

CIP-007

The purpose statement of Reliability Standard CIP-007 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

CIP-007-1 R2 provides:

> 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-Certification to WECC addressing noncompliance with CIP-007-1 R2. Specifically, URE reported it did not adequately evaluate the ports and services to determine whether it had enabled only those ports and services required for normal and emergency operations for Cyber Assets located at six locations.

Initially, URE documented a baseline of all open ports on its system. This baseline was determined based on URE's review of vendor documentation describing expected ports to be open related to running services. However, this review failed to evaluate effectively and document the need for ports and services not identified by the vendor as a potential threat to security. URE identified 19 ports that were enabled without documenting whether they were required for normal and emergency operations. WECC determined that URE failed to establish, document, and implement a process to ensure that it only enabled those ports and services required for normal and emergency operations.

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

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The ports were identified applications on devices that were all located within an Electronic Security Perimeter (ESP). In addition, URE monitors all logical access, and protective boundary devices restrict access. The devices in scope have antivirus and malware prevention tools installed. Finally, URE was aware the 19 ports were open and was actively monitoring the use of the ports.

CIP-007-1 R3

CIP-007-1 R3 provides:

> 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-Certification to WECC addressing noncompliance with CIP-007-1 R3. Specifically, URE reported it failed to apply its patch management program to certain devices located within the ESPs at its facilities. URE failed to track, evaluate, and install 46 security patches released that were applicable to 24 networking devices. Additionally, it failed to track patches for 78 devices comprised of PLCs, emission analyzers, global positioning system (GPS) clocks, chart recorders, thin clients, protocol converters, and switches. WECC determined that because URE was not performing any type of patch tracking on these devices, URE had no way of knowing if or when a patch was released.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, 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 failure to assess security patches could result in vulnerabilities remaining unaddressed for extended periods. This increases the risk of a successful

cyber-attack against CCAs. This increased risk may allow for unauthorized internal and or external access, which could allow for successful cyber-attacks against CCAs essential to operation of the BPS.

Although URE failed to make documentation and records of its security patches available, the devices in scope were all located within an ESP, URE monitored access, and protective boundary devices restricted access. URE stated that the devices in scope have antivirus and malware prevention tools installed and backup procedures in place to limit the duration and exposure of an outage or malicious activity caused by not keeping up to date on patch management.

CIP-007-1 R6

CIP-007-1 R6 provides:

> 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 “Medium” VRF and a “Severe” VSL.

URE submitted a Self-Certification to WECC addressing noncompliance with CIP-007-1 R6. Specifically, URE reported it failed to implement automated tools or organizational process controls to monitor cyber security system events for 83 Cyber Assets within an ESP. URE stated it was unsure if the 83 devices were capable of logging.

WECC determined that URE failed to implement automated tools or organizational process controls to monitor system events related to cyber security for Cyber Assets within the ESP. The 83 devices in scope consisted of PLCs, emission analyzers, GPS clocks, chart recorders, thin clients, and protocol converters, which were not logging access as required.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, 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. All the devices are located within an ESP, URE monitors access, and protective boundary devices restrict access. URE stated that the devices in scope have antivirus and malware prevention tools installed where technically feasible, and backup procedures are in place to limit the duration and exposure of an outage or malicious activity.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred nine thousand dollars ($109,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered certain prior violations in URE's compliance history as aggravating factors in penalty determination;
2. URE was cooperative throughout the compliance enforcement process;
3. URE had an internal compliance program (ICP) at the time of the violations which WECC considered a mitigating factor;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations of CIP-006-1 R1, CIP-007-1 R2, and CIP-007-1 R6 posed a minimal risk to the reliability of the BPS, and the violations of CIP-006-3a R5 and CIP-007-1 R3 posed a moderate risk to the reliability of the BPS, as discussed above;

6. URE submitted to WECC a narrative describing compliance-related improvements URE has made. WECC will review URE's submission and may elect to provide feedback to URE;[5] and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred nine thousand dollars ($109,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[6]

CIP-006-1 R1
URE's Mitigation Plan to address its violation of CIP-006-1 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 WECCMIT008701 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove the HMI monitors from service by disconnecting the Ethernet communications and power sources;
2. change the connection method from Ethernet connections to serial connections, thereby removing these devices from the scope of the NERC CIP Standards; and
3. remove the HMI devices from its CCA list.

URE certified that the above Mitigation Plan requirements were completed.

[5] The narrative described how URE implemented the following changes: 1) URE has developed a process to track deadlines and mitigate violations in a timely manner, thereby minimizing the need for extension requests; 2) URE has created a monthly coordination meeting between compliance groups. This meeting focuses on increasing communication between entities and centralizing issues stemming from information silos; 3) URE has created an annual compliance awareness training program to measure the degree of understanding. URE will include a section to prevent recurrence of NERC Reliability Standard violations; and 4) URE has developed either a process, or improvements to processes, that will help identify the full scope of violations promptly. URE will develop a process for detecting what controls are needed when new devices are installed.
[6] *See* 18 C.F.R § 39.7(d)(7).

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-006-3a R5

URE's Mitigation Plan to address its violation of CIP-006-3a R5 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 WECCMIT009130 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. revise its physical security plan to address unplanned PACM server outages;
2. develop a new procedure to address unscheduled outages;
3. upgrade the PACM system to enable functional hardware redundancy;
4. add procedural controls and requirements for rearming all PSP doors and cabinets and responding during an unscheduled outage; and
5. repair the failed power supply drive and return the system to service.

URE certified that the above Mitigation Plan requirements were completed.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was 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 is designated as WECCMIT009047 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update the ports and services procedure and toolkit. This process includes the following:
    a. work with the vendor to determine the required ports and services;
    b. monitor system operation;
    c. document ports;

d. scan devices to find open/enabled ports;

e. compare results.

2. determine if any unused ports and services require a Technical Feasibility Exception (TFE).

URE certified that the above Mitigation Plan requirements were completed.

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 WECCMIT009048 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. implement a new patch management program and bring patches and security updates to the latest releases; and
2. hold employee workshops and informal discussions to review procedures to let personnel know that patches are applicable to all Cyber Assets within the ESP and not just CCAs.

URE certified that the above Mitigation Plan requirements were completed.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

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 WECCMIT009049-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop a checklist for all assets to determine if the device is capable of logging or if a TFE is needed;
2. perform an assessment of all assets and document what devices are capable of logging to URE's security information and event management database; and

3. file any necessary TFEs.

URE certified that the above Mitigation Plan requirements were completed.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[7]

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,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on January 14, 2014. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred nine thousand dollar ($109,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. WECC considered certain prior violations in URE's compliance history as aggravating factors in penalty determination, as discussed above;
2. URE was cooperative throughout the compliance enforcement process;
3. URE had an ICP at the time of the violations which WECC considered a mitigating factor, as discussed above;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations of CIP-006-1 R1, CIP-007-1 R2, and CIP-007-1 R6 posed a minimal risk to the reliability of the BPS, and the violations of CIP-006-3a and CIP-007-1 R3 posed a moderate risk to the reliability of the BPS, as discussed above;

[7] *See* 18 C.F.R. § 39.7(d)(4).
[8] *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).

6. URE submitted a narrative to WECC describing compliance-related improvements, as discussed above; and
7. 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 nine thousand dollars ($109,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

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

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

b) Record documents for the violation of CIP-006-1 R1, included as Attachment b:
   1. URE's Source Document;
   2. URE's Mitigation Plan designated as WECCMIT008701;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

c) Record documents for the violation of CIP-006-3a R5, included as Attachment c:
   1. URE's Source Document;
   2. URE's Mitigation Plan designated as WECCMIT009130;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

d) Record documents for the violation of CIP-007-1 R2, included as Attachment d:
   1. URE's Source Document;

2. URE's Mitigation Plan designated as WECCMIT009047;
3. URE's Mitigation Plan Extension Request;
4. URE's Certification of Mitigation Plan Completion;

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

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT009048;
3. URE's Mitigation Plan Extension Request;
4. URE's Certification of Mitigation Plan Completion;
5. WECC's Verification of Mitigation Plan Completion;

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

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT009049-2;
3. URE's Mitigation Plan Extension Request;
4. URE's Certification of Mitigation Plan Completion; and
5. WECC's Verification of Mitigation Plan Completion.

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 N. 400 W. Suite 200 Salt Lake City, UT 84103 801-883-6853 jrobb@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	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 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

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 *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