December 31, 2012

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 Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations[3] of CIP-002-1 Requirement (R) 1 and R3, CIP-003-1 R1, CIP-004-1 R2 and R4, CIP-005-1 R1, CIP-006-2 R1, CIP-007-1 R1 and R3, PRC-005-1 R2, PRC-008-0 R2 and VAR-002-1.1b R3.[4] According to the Settlement Agreement, URE agrees that with

[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.

[4] The violations of CIP-003-1, CIP-004-1 and CIP-005-1 span versions 1 through 2 of the Standard. For consistency, version 1 will be referenced throughout the Notice of Penalty. The violations of CIP-002-1 span versions 1 through 3 of the Standard. For consistency, version 1 will be referenced throughout the Notice of Penalty. The violation of CIP-006-2 R1 spans versions 2 through 3a of the Standard. For consistency, version 2 will be referenced throughout the Notice of Penalty. The violation of CIP-007-1 R3 spans versions 1 through 2a of the Standard. For consistency, version 1 will be referenced throughout the

two exceptions, the violations addressed therein may be treated as Confirmed Violations pursuant to the NERC Rules of Procedure and has agreed to the assessed penalty of two hundred seven thousand dollars ($207,000), 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. URE neither admits nor denies the Violations of CIP-002-1 R1 and CIP-007-1 R1. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201002301, WECC201002302, WECC201002303, WECC201002305, WECC201002306, WECC201002307, WECC201002308, WECC201002310, WECC201002311, WECC201102539, WECC201102537 and WECC201002373 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, by and between WECC and URE, which is included as Attachment a. The details of the findings and the 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 (2012), 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	Unidentified	NOC-1702	WECC201002301	CIP-002-1	R1	Medium[5]	$207,000

Notice of Penalty. The violation of PRC-005-1 spans versions 1 through 1b of the Standard. For consistency, version 1 will be referenced throughout the Notice of Penalty.

[5] CIP-002-1 R1 and R1.2 each have a "Medium" Violation Risk Factors (VRF); CIP-002-1 R1.1, R1.2.1, R1.2.2, R1.2.3, R1.2.4, R1.2.5, R1.2.6 and R1.2.7 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-002-1 R1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower "VRF for CIP-002-1 R1 was in effect from June 18, 2007 until January 27, 2009 when the "Medium" VRF became effective.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Electricity Coordinating Council	Registered Entity		WECC201002302	CIP-002-1	R3	High[6]	
			WECC201002303	CIP-003-1	R1/R1.2	Lower[7]	
			WECC201002305	CIP-004-1	R2/R2.1/ R2.2/R2.3	Medium[8]	
			WECC201002306	CIP-004-1	R4	Medium[9]	
			WECC201002307	CIP-005-1	R1	Medium[10]	
			WECC201002308	CIP-006-2	R1	Medium[11]	
			WECC201002310	CIP-007-1	R1	Medium[12]	
			WECC201002311	CIP-007-1	R3	Lower	

[6] CIP-002-1 R3 has a "High" VRF; CIP-002-1 R3.1. R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-002-1 R3 a "Medium" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "High" VRF and on January 27, 2009, the Commission approved the modified "High" VRF. Therefore, the "Medium" VRF for CIP-002-1 R3 was in effect from June 18, 2007 until January 27, 2009 when the "High" VRF became effective.

[7] CIP-003-1 R1 has a "Medium" VRF; CIP-003-1 R1.1, R1.2 and R1.3 each have a "Lower" VRF. In the context of this case, WECC determined the violation related to R1.2 and a "Lower" VRF was appropriate. When NERC filed VRFs it originally assigned CIP-003-1 R1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[8] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" VRF; CIP-004-1 R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. In the context of this case, WECC determined the violation related to R2.1, R2.2 and R2.3, and a "Medium" VRF was appropriate. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[9] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; CIP-004-1 R4.2 has a "Medium" VRF. In the context of this case, WECC determined the violation related to R4.1 and R4.2 and a "Medium" VRF was appropriate. When NERC filed VRFs, it originally assigned CIP-004-1 R4.2 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R4.2 was in effect from June 18, 2007 until January 27, 2009 when the "Medium" VRF became effective.

[10] CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a "Medium" VRF; CIP-005-1 R1.6 has a "Lower" VRF.

[11] CIP-006-2 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; CIP-006-2 R1.7 and R1.8 each have a "Lower" VRF.

[12] CIP-007-1 R1 and R1.1 each have a "Medium" VRF; CIP-007-1 R1.2 and R1.3 each have a "Lower" VRF.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
			WECC201102539	PRC-005-1	R2	High[13]	
			WECC201102537	PRC-008-0	R2	Medium	
			WECC201002373	VAR-002-1.1b	R3	Medium	

WECC201002301 CIP-002-1 R1

The purpose statement of Reliability Standard CIP-002-1 provides:

> NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities[14] should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment. Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.
>
> Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

[Footnote added.]

[13] PRC-005-1 R2 has a "Lower" VRF; PRC-005-1 R2.1 and R2.2 each have a "High" VRF. In the context of this case, WECC determined the violation related to R2.1 and a "High" VRF was appropriate. During a final review of the standards subsequent to the March 23, 2007 filing of the Version 1 VRFs, NERC identified that some standards requirements were missing VRFs; one of these include PRC-005-1 R2.1. On May 4, 2007, NERC assigned PRC-005 R2.1 a "High" VRF. In the Commission's June 26, 2007 Order on Violation Risk Factors, the Commission approved the PRC-005-1 R2.1 "High" VRF as filed. Therefore, the "High" VRF was in effect from June 26, 2007. The Settlement Agreement on page 41 incorrectly states a VRF of "Medium." "High" is the correct VRF assessment.

[14] Within the text of Standard CIP-002 through CIP-007, "Responsible Entity" shall mean Reliability Coordinator, BA, Interchange Authority, TSP, TO, TOP, GO, GOP, LSE, NERC, and Regional Reliability Organizations.

CIP-002-1 R1 provides:

> R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.
>
> R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
>
> R1.2. The risk-based assessment shall consider the following assets:
>
> R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.
>
> R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.
>
> R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.
>
> R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.
>
> R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.
>
> R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.
>
> R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

CIP-002-1 R1 has a "Medium" VRF and a "Severe" Violation Severity Level (VSL).

WECC conducted a Compliance Audit of URE. WECC reviewed URE's risk-based assessment methodology (RBAM) and found that URE was in violation of CIP-002-1 R1. Specifically, URE's RBAM failed to include descriptions of procedures and criteria as required by R1.1. In addition, the RBAM did not consider all assets as required by R1.2. WECC determined that URE failed to demonstrate that it had documented an RBAM that fully complied with all the elements of CIP-002-1 R1. WECC Enforcement determined that URE's RBAM did not describe in sufficient detail all of the procedures and criteria used by URE to identify Critical Assets as required under R1.1. In addition, URE had not clearly demonstrated in its RBAM documentation that it had assessed all assets required to be considered under R1.2.

WECC determined that the violation lasted from the date the Standard became mandatory and enforceable to URE, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS) because of the following mitigating factors. In this case, risks posed by URE's noncompliance with CIP-002-1 R1.1 were limited in that the violation stems from documentation that failed to adequately describe URE's RBAM criteria and procedure used to identify Critical Assets. Evidence reviewed by WECC demonstrates that URE's implementation of its RBAM did include criteria and procedures used to identify Critical Assets that were not included in the RBAM documentation. Based on WECC's investigation, the risks posed by URE's noncompliance are, to some extent, lessened in that URE did document and implement a RBAM that resulted in identification of all its Critical Assets, including substations and control centers. Although URE may not have provided documentation evidencing compliance under R1, WECC's discussion with URE staff indicates that URE's corporate security policy provides protections that constitute compensating measures, thereby reducing the BPS risk. Specifically, the Critical Assets were all located within Physical Security Perimeters (PSPs) and Electronic Security Perimeters (ESPs) where physical access to the devices were controlled and monitored. In addition, all employees had personnel risk assessments (PRAs). Furthermore, unauthorized access attempts would have been alarmed. WECC also determined that the risks presented by URE's failure to consider all assets listed under R1.2 were limited, in that many transmission assets critical to system restoration and blackstart were identified as Critical Assets to the BPS based on size and interconnectivity pursuant to R1.2.2.

WECC201002302 CIP-002-1 R3

CIP-002-1 R3 provides:

> R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> > R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
> >
> > R3.2. The Cyber Asset uses a routable protocol within a control center; or,
> >
> > R3.3. The Cyber Asset is dial-up accessible.

CIP-002-1 R3 has a “High” VRF and a “Severe” VSL.

WECC conducted a Compliance Audit of URE. During the course of the Audit, WECC auditors determined that URE failed to identify all Critical Cyber Assets (CCAs) associated with identified Critical Assets in violation of CIP-002-1 R3. Specifically, WECC auditors determined that URE failed to identify a system control center workstation as a CCA. Shortly after the conclusion of the on-site Audit, URE self-reported a violation of CIP-002-1 R3 that expanded the scope of the noncompliance identified at the Audit. Specifically, URE reported that it failed to identify eight CCAs associated with a certain facility. WECC Enforcement reviewed the audit report, WECC auditor findings and URE's responses to audit data requests. WECC Enforcement also reviewed additional information submitted by URE post-audit and URE's Self-Report. Based on this review, WECC Enforcement determined that URE failed to identify all CCAs associated with Critical Assets. More specifically, URE failed to identify the following CCAs: 1) an energy management system (EMS) workstation that allows for system control and monitoring and uses a routable protocol within URE’s primary control center; 2) eight computer devices, which are identified as Critical Assets; and 3) a CCA associated with a substation.

WECC determined that URE had a violation of CIP-002-1 R3 because URE failed to identify all CCAs associated with Critical Assets as required by CIP-002-1 R3.

WECC determined that the violation lasted from the date the Standard became mandatory and enforceable to URE, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS because of the following mitigating factors. The scope of the CIP-002-1 R3 violation is limited to ten devices that were all located within ESPs and PSPs. These devices were, therefore, afforded a number of protections required under the CIP Standard Requirements.

The devices were physically secured during the violation period. All of the devices in scope were located within PSPs per CIP-006-1. Physical access was restricted to individuals with specific authorization per CIP-006-1 R1. Individuals with authorized access completed PRAs and cybersecurity training per CIP-004-1 R2 and R3. Access to the devices through the PSP was controlled using card keys, and security personnel consistent with CIP-006-1 R2. Furthermore, physical access to the devices was monitored. There were no unauthorized physical access attempts. Nevertheless, unauthorized physical access attempts at PSP access points would have triggered alarms per CIP-006-1 R3. Access to the devices was logged at PSP access points per CIP-006-1 R4.

The devices were also electronically secured. As stated above, each of the ten devices was located within ESPs. Each ESP limited access to authorized individuals. Individuals with electronic access completed PRAs and cybersecurity training per CIP-004-1 R2 and R3. Access at all electronic access points was controlled using technical and procedural mechanisms. Authorization was granted per the process outlined under CIP-005-2 R2. Access to the ESPs was denied by default. Electronic access was monitored 24-hours a day, 7 days a week per CIP-005-1 R3. Unauthorized electronic access attempts would have triggered alarming. Only ports and services required for normal and emergency operations were enabled on the devices per CIP-007-1 R2. Devices were secured using anti-virus software where technically feasible per CIP-007-1 R4. Access to accounts provisioning access to the devices was controlled per CIP-007-1 R5 through the use of passwords and “need to know” access grants. Cybersecurity events that occurred within ESPs were monitored and would have triggered alarming as described in CIP-007-1 R6.

WECC201002303 CIP-003-1 R1

The purpose statement of Reliability Standard CIP-003-1 provides: “Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber

Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-003-1 R1 provides:

> R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:
>
> > R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
> >
> > R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
> >
> > R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

CIP-003-1 R1 has a "Lower" VRF and a "Severe" VSL.

WECC issued its Audit Notice to URE, notifying URE that WECC would be conducting an on-site Compliance Audit. Two weeks before the Audit, URE self-reported a violation of CIP-003-1 R1. Specifically, URE reported that it failed to make its cybersecurity policy readily available to 52 contractors with unescorted physical access to CCAs. In addition, URE reported that the policy was not made readily available to 14 interconnected entity's employees with unescorted physical access to one URE substation control house containing CCAs.

During the course of the on-site Audit, WECC auditors investigated the distribution of URE's cybersecurity policy and determined that URE failed to make its cybersecurity policy readily available to contractors and contract personnel supporting URE's EMS. Although the policy was available to URE personnel on URE's intranet site, the policy was not made available to approximately 66 individuals who did not have access to the intranet site but who had unescorted physical access to CCAs.

WECC Enforcement reviewed the Audit Report and URE's Self-Report. Based on this review and its own analysis, WECC Enforcement determined that URE failed to comply with CIP-003-1 R1 because URE failed to make its cybersecurity policy available to all personnel with access to CCAs. Although URE made its cybersecurity policy available on its intranet site, access was limited to URE employees

with electronic access to the intranet site. Consequently, 66 contractors and personnel did not have access to URE's cybersecurity policy for a two-year period.

WECC determined that the violation lasted from the date the Standard became mandatory and enforceable to URE, through when URE made its cybersecurity policy available for all individuals with access to CCAs.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. All individuals with unescorted physical access to CCAs completed PRAs and cybersecurity training. Further, all physical access to CCAs was monitored and controlled by URE. The scope of the violation is limited, in that the policy was made available to the majority of individuals with access to CCAs.

WECC201002305 CIP-004-1 R2

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

> 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 R2 provides:

> R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
>
> > R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.
> >
> > R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

CIP-004-1 R2 has a "Medium" VRF and a "Moderate" VSL.

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process. One day before the Self-Certification was due, URE submitted a Self-Report citing possible noncompliance with CIP-004-1 R2.1, R2.2 and R2.3. URE submitted its Self-Certification, referencing the noncompliance cited in its Self-Report. Pursuant to WECC's Audit Notice issued to URE, WECC conducted an on-site Audit of URE compliance with CIP Reliability Standards. During the course of the Audit, WECC auditors investigated noncompliance reported by URE in its Self-Report and Self-Certification. As reported by URE, auditors also determined that URE failed to comply with R2.1, R2.2 and R2.3. Auditors cited URE in possible violation of CIP-004 R2 and forwarded their findings to WECC Enforcement. WECC Enforcement reviewed URE's Self-Report, Self-Certification and the Audit findings citing noncompliance with CIP-004-1 R2. WECC Enforcement determined that URE failed to document and implement a security training program that fully complied with CIP-004-1 R2 and its subrequirements, R2.1, R2.2 and R2.3, in the following manner.

URE self-reported that 31 individuals did not complete training within 90 days of receiving cyber access to CCAs, in violation of CIP-004-1 R2.1. WECC found that on 29 individuals were given cyber access to CCAs located in URE's control center. These individuals were required per R2.1 to complete training three months later; however, they did not receive the training until five months or seven months later. There were an additional two individuals who were not trained within the 90-day period prescribed by R2.1. They received cyber access to the CCAs but did not complete the training until 115 and 210 days, respectively, after cyber access to CCAs was granted.

URE also self-reported the violation of CIP-004-1 R2.2. WECC reviewed URE's training program for all personnel with authorized cyber and/or unescorted physical access to CCAs. WECC found that URE's training program for personnel with cyber and physical access to CCAs had the requirements of R2.2; however, personnel with only unescorted physical access to CCAs were trained under a different program that did not include all the criteria required by R2.2. In total, 55 individuals with physical access to CCAs did not receive training as required by R2.2.

During the Audit, WECC determined that URE failed to maintain documentation of annual training as required by R2.3 for 48 personnel with unescorted physical access to CCAs. URE reported that the 48 individuals did not complete annual re-training as required by the Standard. The individuals did complete annual training the previous year and had current PRAs. Access for 2 individuals who did not complete annual re-training was revoked. In addition to the 48 individuals reported by URE, WECC identified 3 additional personnel with physical access rights who did not receive or complete annual re-training.

WECC determined that URE was in violation of CIP-004-1 R2 for failing to: 1) ensure personnel granted cyber and physical access to CCAs received training within the period prescribed by 2.1, as well as by failing to revoke access rights after 90 days for personnel who did not receive training; 2) ensure personnel with physical access to CCAs received training as required by R2.2; and 3) document a cybersecurity training program that complied with R2.3.

WECC determined that the violation lasted from the date the Standard became mandatory and enforceable to URE, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. URE ensured that all personnel with access to CCAs completed a PRA. In addition, although URE's program did not strictly adhere to CIP-004-1 R2.2, URE did provide training that familiarized personnel with CIP security and CCA access procedures. Personnel with only physical access receiving physical access training and personnel with only electronic access received electronic access training. The training included instruction on proper use of CCAs, as well as the proper handling of CCA information.

WECC201002306 CIP-004-1 R4

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 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.
> >
> > 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 "Medium" VRF and a "Moderate" VSL.

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process. One day before the Self-Certification was due, URE self-reported a CIP-004-1 R4 violation. Specifically, URE reported that for an 11-day period, it did not include all applicable employees in its access list pursuant to R4. Further, URE reported that it discovered that access rights held by an interconnected entity's employee were not revoked when the employee retired ten months earlier, as required by R4.2.

WECC determined that URE failed to maintain and update access lists pursuant to R4.1. Specifically, URE failed to list four personnel granted unescorted physical access to CCAs. Physical access granted to these individuals was limited to CCAs located within a Critical Asset substation. Although these four individuals completed required training and PRAs, URE security personnel failed to update substation and master access lists after the four personnel were granted physical access.

URE submitted a separate Self-Report 17 months later, indicating that a URE employee at a certain facility had access to a shared operator password and was not documented on the access list, as required under CIP-004-1 R4. The access list should have reflected this employee's access, but his

name was inadvertently left off the access list. The plant manager confirmed the employee had been authorized to use the password, had a completed PRA and received CIP training.

In addition to URE's failure to update lists with personnel granted physical access rights, WECC determined that URE failed to maintain access lists for contractors and service vendors pursuant to R4.1. URE reported that during the course of its quarterly review of access lists, URE security personnel identified a contractor, the interconnect entity's employee who retired but who remained on the substation access list of contractors with physical access to CCAs.

Although URE confiscated the retired contractor's access badge, thereby removing his physical access to CCAs, URE did not update its access lists to reflect access revocation by the effective date of the Standard. URE security personnel identified the retired contractor in its access lists. After URE security personnel verified that the contractor's access badge was taken prior to his retirement, it updated its personnel access lists and removed the contractor as a person with authorized physical access to CCAs.

WECC also determined that URE had a violation of R4.2. In two instances, URE personnel were granted unescorted physical access for one day only, but actually received access that did not terminate at the conclusion of the day. In addition, WECC determined that the two individuals used the granted access multiple times after that day. Six weeks later, URE security personnel detected and revoked access for these two individuals. URE did not remove temporary access rights within seven days for these two individuals, in violation of CIP-004-1 R4.2. WECC confirmed, however, that URE detected and revoked ongoing temporary access.

WECC determined that URE had a violation of R4.1 for failing to list all personnel granted cyber access or authorized unescorted physical access rights to CCAs. WECC also determined that URE had a violation of R4.2 for failing to revoke access rights within 24 hours for personnel terminated for cause or within seven calendar days for personnel who no longer required access to CCAs.

WECC determined that the violation, as related to R4.1, lasted from the date the Standard became mandatory and enforceable, through when URE removed the contractor from the personnel access lists. WECC determined the duration of the violation, as related to R4.2, to be from the date the two individuals were granted unescorted access to CCAs and the access was not terminated at the conclusion of that day, through when URE revoked the two individuals' access.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. Although URE did not update lists to reflect changes in personnel with access to CCAs, URE did remove these individuals' access rights. Further, for the two individuals granted

temporary access that was not revoked within seven days pursuant to R4.2, URE ensured that these individuals did complete CCA training and had completed PRAs.

WECC201002307 CIP-005-1 R1

The purpose statement of Reliability Standard CIP-005-1 provides, in pertinent part: "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:

> 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 "Lower" VSL.

WECC conducted a Compliance Audit of URE. During the course of the Audit, WECC identified Cyber Assets, involved in ESP access control and monitoring, that were not afforded protective measures prescribed by R1.5. Specifically, URE's specific servers are Cyber Assets used for ESP access authentication for control center CCAs. These servers were not identified or protected as Cyber Assets used for ESP access control and monitoring pursuant to R1.5. WECC determined that URE failed to identify and secure two Cyber Assets used to monitor remote access to ESPs encompassing CCAs associated with its control center and backup control center.

WECC determined that URE had a violation of CIP-005-1 R1 for failing to afford Cyber Assets used in the access control and monitoring of the ESP the protective measures required by R1.5.

WECC determined that the violation lasted from the date the Standard became mandatory and enforceable to URE, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS because of a number of compensating factors unique to URE's cyber network. URE's layered security consisted of dial-up accessible devices protected by cryptographic modems. Further, URE had a strong authentication system in place.

WECC201002308 CIP-006-2 R1

The purpose statement of Reliability Standard CIP-006-2 provides: "Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2."

CIP-006-2 R1 provides:

> R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R.1.1 All Cyber Assets within an Electronic Security Perimeter shall 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 such Cyber Assets.
> >
> > R1.2. Identification of all physical 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. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
> >
> > R1.5**.** Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.
> >
> > R1.6. Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.
> >
> > R1.7. Update of the physical security plan within thirty calendar days of the completion 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.
> >
> > R1.8**.** Annual review of the physical security plan.

CIP-006-2 R1 has a "Medium" VRF and a "Moderate" VSL.

WECC conducted a Compliance Audit of URE. WECC toured portions of URE's facility. WECC determined that URE failed to identify one access point to a PSP. Specifically, the designated PSP could be accessed via an emergency escape hatch, approximately three feet by three feet in size. Although the hatch did have a cover, the cover was neither locked nor alarmed to detect or deter unauthorized access attempts to the PSP. WECC determined that URE failed to implement a physical security plan (Plan) that included processes to ensure identification of all access points through each PSP pursuant to R1.2.

URE self-reported a violation of CIP-006-2 R1.6. On a single day, URE failed to provide continuous escorted access of a visitor within the PSP, in violation of CIP-006-2 R1.2. The visitor was a vendor who had been performing work at the specific site for several years and was inside the PSP for approximately ten minutes. WECC determined that URE was in violation of CIP-006-2 R1. Specifically, URE failed to identify and secure a PSP access point, in violation of CIP-006-2 R1.2. WECC also determined that URE failed to provide continuous escorted access to the vendor within a PSP for approximately ten minutes.

WECC determined that URE was in violation of CIP-006-2 R1 for failing to identify and secure all PSP access points pursuant to R1.2 and failing to provide continuous escorted visitor access within a PSP pursuant to R1.6.

WECC determined that the violation lasted from the day following Certification of Mitigation Plan Completion for a prior violation, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. The risks of URE's failure to identify a single access point are lessened by layered security measures implemented at the facility. Two card key controlled vehicle access gates, a water boundary and rough terrain provide deterrents to unauthorized entry. Further, two physical security cameras located on the exterior provide 24-hours a day, 7 days a week monitoring for the identified PSP access point.

WECC201002310 CIP-007-1 R1

The purpose statement of Reliability Standard CIP-007-1 provides, in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-007-1 R1 provides:

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

CIP-007-1 R1 has a "Medium" VRF and a "Severe" VSL.

WECC conducted a Compliance Audit of URE. WECC found that URE was in violation of CIP-007-1 R3 for failing to establish and maintain a cybersecurity test procedure that minimized adverse effects on the production system. The basis for WECC's determination stems from URE's testing procedure and testing documentation in place for a 12-month period. The WECC auditors determined that testing procedure documentation in effect during this period was limited to EMS CCAs. In addition to discussing documentation with URE, WECC reviewed documentation to assess URE's compliance with CIP-007-1 R1.

Beyond URE's assurances that a testing procedure was maintained through institutional knowledge, WECC determined documentation produced by URE did not constitute a testing procedure pursuant to CIP-007-1 R1. The documentation did not outline a process to be followed. Further, it did not clearly identify the circumstances triggering a cybersecurity test, nor did it include all Cyber Assets within an ESP. Although WECC determined that URE's test procedure document appeared to provide a procedure consistent with CIP-007-1 R1.1, this process was not in effect until 12 months after the compliance enforcement date. WECC determined that URE did not have a testing procedure that complied fully with CIP-007-1 R1 on the compliance enforcement date. Specifically, URE failed to create and implement test procedures to assess significant changes to all CCAs per R1.1 and to provide

documentation of testing per R1.2 and R1.3. Although the documentation addressed patching for the EMS, the template did not reference any other testing triggered by the other significant changes outlined in R1. Most notably, it did not include test procedures to ensure that new Cyber Assets and all significant changes to existing Cyber Assets within the ESP did not affect existing cybersecurity controls.

WECC determined that URE had violated CIP-007-1 R1 for failing to establish and maintain a cybersecurity test procedure that minimized adverse effects on the production system.

WECC determined that the violation lasted from the date the Standard became mandatory and enforceable to URE, through when URE created and implemented cybersecurity test procedures per CIP-007-1 R1.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. URE maintains that although its documentation for a one-year period was incomplete, it assessed and tested significant changes to Cyber Assets in its EMS environment. Further, during on-site interviews with URE subject matter experts (SMEs), WECC confirmed testing was performed during the violation period.

WECC201002311 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 "High" VSL.

WECC notified URE that it would be conducting an on-site Audit of URE compliance with NERC CIP Reliability Standards. The following month, URE self-reported a violation of CIP-007-1 R3 and CIP-007-2 R3 at a specific facility. URE discovered that it failed to assess and update its anti-virus software at the facility within the timeframe prescribed under CIP-007-1 R3. URE's Self-Report applied to all human-machine interfaces (HMIs) within ESPs at a specific facility, all of which are designated as CCAs.

WECC determined that URE had a violation of CIP-007-1 R3 for failing to assess and update its anti-virus software within 30 days of availability.

WECC determined that the violation lasted from the date the anti-virus software was available, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. URE was able to demonstrate that it established and documented a program pursuant to R3 and, with the exception of the anti-virus software used on HMIs at the facility, it did assess and implement patches for other Cyber Assets and CCAs. Further, the facility has a supervisory control and data acquisition (SCADA) network that is isolated from URE's LAN/corporate network, protective relay, physical security network and any Internet access. The facility's ultimate defense against cyber incidents coming from the Internet is that the network is separated by an air gap. Due to the existing air gap, the SCADA network was likely not susceptible to the vulnerabilities protected against in the anti-virus program update. During the violation period, the facility did not have any cyber incidents affecting normal operations of the SCADA network.

WECC201102539 PRC-005-1 R2

The purpose statement of Reliability Standard PRC-005-1 provides: "To ensure all transmission and generation Protection Systems[15] affecting the reliability of the Bulk Electric System (BES) are maintained and tested."

[Footnote added.]

[15] *The NERC Glossary of Terms Used in Reliability Standards* defines Protection System as "Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry."

PRC-005-1 R2 provides in pertinent part:

> R2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization[16] on request (within 30 calendar days). The documentation of the program implementation shall include:
>
> > R2.1. Evidence Protection System devices were maintained and tested within the defined intervals.
>
> [Footnote added.]

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

WECC conducted a Compliance Audit of URE. WECC's audit team reviewed URE's Protection System maintenance and testing program (Program), as well as evidence of maintenance and testing records disclosed by URE. In a response to WECC's data request for evidence of substation maintenance and testing records, URE submitted a response, but also self-reported a violation of PRC-005-1 R2 two days later. In both the response and the Self-Report, URE disclosed that annual testing tasks were not completed for any substation batteries subject to PRC-005-1 as prescribed under URE's Program. URE also stated it was not completing certain semi-annual testing tasks for one type of battery. Based on its review of testing and maintenance records, the WECC audit team determined that URE failed to demonstrate that it performed certain annual and semi-annual testing for substation batteries. In addition, the WECC audit team determined that URE failed to provide evidence of annual maintenance and testing for communication devices. In addition, URE failed to provide evidence of previous test dates for 65 percent of communication devices. The WECC audit team forwarded its findings to WECC Enforcement.

Consistent with the WECC audit team findings, WECC Enforcement found that URE was in violation of PRC-005-1 for failing to provide evidence of annual testing for all substation batteries subject to the Standard. WECC Enforcement also found that URE failed to provide evidence of semi-annual maintenance and testing for a certain type of batteries constituting ten percent of substation batteries subject to maintenance and testing under URE's Program, as required by the Standard. WECC

[16] Consistent with applicable FERC precedent, the term "Regional Reliability Organization" in this context refers to WECC.

Enforcement did, however, determine that the scope of the violation did not include communication devices. URE's Program prescribes a six-year interval for communication equipment. URE staff disclosed in its interview with the WECC audit team that in addition to maintenance and testing on a six-year interval, many communication devices were tested annually. WECC Enforcement determined that although URE staff performed maintenance and testing on many communication devices on an annual basis, compliance with PRC-005-1 R2 requires URE to produce evidence of maintenance and testing in accordance with the six-year interval prescribed by URE's Program. WECC Enforcement reviewed URE records, and determined that URE did perform maintenance and testing of communication equipment in accordance with the six-year interval prescribed by its Program. WECC Enforcement, therefore, determined that the scope of the violation does not include communication devices.

WECC determined that URE had a violation of PRC-005-1 for failing to provide evidence of annual and semi-annual battery maintenance and testing.

WECC determined that the violation lasted from the day following Certification of Mitigation Plan Completion for a prior violation, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. The risk was offset by URE's maintenance of other Protection System equipment, and the fact that, with regard to batteries, URE did provide evidence of monthly testing. Further, although URE failed to perform semi-annual maintenance and testing on certain batteries, these batteries account for ten percent of URE substation batteries subject to PRC-005-1. For the majority of substation batteries, approximately 90 percent, URE provided evidence of semi-annual maintenance and testing as prescribed under its Program. Because maintenance and testing tasks required at annual and semi-annual intervals are similar, evidence of semi-annual testing for 90 percent of its substation batteries offset the risk posed by URE's noncompliance.

WECC201102537 PRC-008-0 R2

The purpose statement of Reliability Standard PRC-008-0 provides: "Provide last resort system preservation measures by implementing an Under Frequency Load Shedding (UFLS) program."

PRC-008-0 R2 provides: "The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days)."

PRC-008-0 R2 has a "Medium" VRF and a "Severe" VSL.

WECC conducted a Compliance Audit of URE. WECC's audit team reviewed URE's list of UFLS relays and station batteries for its UFLS facilities. The audit team also reviewed the maintenance and testing program for UFLS equipment as defined in URE's UFLS procedures.

The audit team issued a data request for evidence of semi-annual and annual substation UFLS battery maintenance and testing records. In its response, URE provided maintenance and testing records, but stated that it failed to complete all interval maintenance and testing for batteries. WECC SMEs reviewed URE's response and determined that URE records did not demonstrate that testing and maintenance was performed on a semi-annual and annual basis for all batteries. Specifically, WECC SMEs determined that URE failed to complete semi-annual maintenance and testing for certain batteries comprising approximately ten percent of URE batteries included in its UFLS Program. Further, WECC SMEs determined that URE failed to complete annual maintenance tasks for all batteries subject to its UFLS maintenance and testing plan.

URE self-reported a violation of PRC-008-0 R2. URE's Self-Report cited the issues identified by the audit team and initially disclosed by URE in its data request response. During the course of the Audit, WECC SMEs reviewed the Self-Report and determined that it was identical in scope to the Audit findings. The WECC SMEs determined that URE was in violation of PRC-008-0 R2 and forwarded their findings to WECC Enforcement.

WECC Enforcement reviewed the audit team findings as well as URE's Self-Report. WECC Enforcement determined that URE failed to perform semi-annual maintenance and testing for certain batteries and annual maintenance and testing for all batteries included in its UFLS program.

WECC determined that URE had a violation of PRC-008-0 R2 for failing to implement UFLS battery maintenance and testing as required by the Standard.

WECC determined that the violation lasted 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 a serious or substantial risk to the reliability of the BPS. URE provided evidence demonstrating monthly maintenance and testing, as well as completion of its five-year battery discharge tests for all batteries subject to the Standard. Further, WECC determined that although URE failed to complete semi-annual testing for certain batteries, URE

did complete semi-annual testing for all other types, including 90% of substation batteries included in the UFLS Program.

WECC201002373 VAR-002-1.1b R3

The purpose statement of Reliability Standard VAR-002-1.1b provides: "To ensure generators provide reactive and voltage control necessary to ensure voltage levels, reactive flows, and reactive resources are maintained within applicable Facility Ratings to protect equipment and the reliable operation of the Interconnection."

VAR-002-1.1b R3 provides:

> R3. Each Generator Operator shall notify its associated Transmission Operator as soon as practical, but within 30 minutes of any of the following:
>
> > R3.1. A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.
> >
> > R3.2. A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.

VAR-002-1.1b R3 has a "Medium" VRF and a "Severe" VSL.

URE self-reported a violation of VAR-002-1.1b R3. Specifically, URE reported that on a single day, at approximately 12:19 a.m., the power system stabilizer (PSS) was deactivated at a certain facility unit. URE reported that the PSS was returned to service later that day, at 7:45 a.m. URE reported, however, that it failed to notify the TOP within 30 minutes of the PSS status change and the expected duration of the PSS deactivation. URE notified the TOP of the PSS status change at 4:26 p.m., 14 hours and seven minutes after the PSS was initially removed from service. WECC determined that URE failed to issue notice to its TOP within 30 minutes of a PSS status change, in violation of VAR-002-1.1b R3.

WECC determined that the violation lasted one day, from the date URE failed to notify the TOP of the change in the status of its PSS, to several hours later, when URE gave notice of PSS status to its TOP.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. The instant violation is limited to one PSS. Further, although the PSS was removed from service, the voltage for the transmission system was monitored and controlled by the GOP, consistent with the required voltage schedule.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two hundred seven thousand dollars ($207,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. URE received self-reporting credit for the CIP-002-1 R3, CIP-003-1 R1, CIP-007-1 R3 and VAR-002-1.1b R3 violations;[17]
2. URE did not receive self-reporting credit for the CIP-004-1 R2 and R4 violations since it self-reported during the Self-Certification period;
3. URE did not receive self-reporting credit for the PRC-005-1 R2 and PRC-008-0 R2 violations since it self-reported after the WECC audit team had already identified the violations;
4. WECC reviewed URE's internal compliance program (ICP) and considered it a mitigating factor in penalty determination;
5. URE was cooperative throughout the compliance enforcement process;
6. URE did not fail to complete any applicable compliance directives;
7. There was no evidence of any attempt by URE to conceal the violations;
8. There was no evidence that URE's violations were intentional; and
9. WECC considered as an aggravating factor some elements of URE's violation history.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of two hundred seven thousand dollars ($207,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

[17] While URE self-reported the CIP-002-1 R3 violation in the face of an Audit, WECC applied mitigating credit since URE voluntarily disclosed additional instances of noncompliance that were not identified at the Audit. In addition, while URE self-reported the CIP-007-1 R3 violation in the face of an Audit, WECC applied mitigating credit since URE supplied useful information in the resolution of the matter.

Status of Mitigation Plan[18]

WECC201002301 CIP-002-1 R1
URE's Mitigation Plan to address its violation of CIP-002-1 R1 was submitted to WECC on May 31, 2012. The Mitigation Plan was accepted by WECC on July 11, 2012 and approved by NERC on August 7, 2012. The Mitigation Plan for this violation is designated as WECCMIT007445 and was submitted as non-public information to FERC on August 7, 2012 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revise its RBAM and any other relevant documentation to include clear procedures and evaluation criteria used to assess and identify Critical Assets pursuant to all requirements and subrequirements under CIP-002-1; and
2. Make clear in this revised documentation that it does, in fact, consider all assets required to be considered by the Standard.

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

1. Annual RBAM document; and
2. Critical Asset assessment form template.

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

WECC201002302 CIP-002-1 R3
URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to WECC. WECC issued a notice of Mitigation Plan rejection and request for revision. URE submitted a revised Mitigation Plan to include the expanded scope of the violation and mitigation action required for eight Cyber Assets. URE submitted a second revised Mitigation Plan. WECC reviewed this revised Mitigation Plan and determined that the Mitigation Plan did not address the full scope of the violation as described in the Notice of Alleged Violation. Further, URE requested an extension to the Mitigation Plan completion date contained in the revised Mitigation Plan. WECC issued a notice of Mitigation Plan rejection. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by WECC on March 2, 2012 and approved by NERC on March 26, 2012. The Mitigation Plan for this violation is designated as

[18] *See* 18 C.F.R § 39.7(d)(7).

WECCMIT006658 and was submitted as non-public information to FERC on March 26, 2012 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Add the device identified during the Audit to the CCA list and apply any additional protective measures required to bring the asset into full compliance as a CCA;
2. Add the computer device assets at the facility that were not on the CCA list and apply any additional protective measures required to bring those assets into full compliance as CCAs;
3. Verify that the computer device at the substation has been identified as a CCA following all NERC CIP requirements (these include proposed Technical Feasibility Exceptions (TFEs));
4. Install a managed switch at the substation and identify as an access point to the ESP. All NERC CIP requirements will be followed and documented (these include proposed TFEs);
5. Redefine the ESP to include the newly-identified CCA and access point;
6. Update all documentation to reflect substation changes;
7. Review and update vulnerability assessment procedures to ensure a more accurate assessment of facilities;
8. Implement training on the updated procedures; and
9. Provide evidence of the assessment of all Critical Assets for any CCAs essential to their operation under R3. This evidence will include "null lists" for Critical Assets that have no associated CCAs.

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 verified that URE's Mitigation Plan was completed.

WECC201002303 CIP-003-1 R1

URE's Mitigation Plan to address its violation of CIP-003-1 R1 was submitted to WECC on August 30, 2010. The Mitigation Plan was accepted by WECC on September 21, 2011 and approved by NERC on October 19, 2011. The Mitigation Plan for this violation is designated as WECCMIT004326 and was submitted as non-public information to FERC on October 20, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Make hard copies of its cybersecurity policy readily available in work areas of personnel with unescorted physical access to CCAs;
2. Provide its cybersecurity policy to the outside vendor supporting its EMS;
3. Provide its cybersecurity policy to an interconnected entity for employees with access to URE CCAs in URE substations containing this interconnected entity-owned equipment.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted attestations that action was completed, specifically that copies of the cybersecurity policy were distributed to the parties listed above.

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

WECC201002305 CIP-004-1 R2

URE's Mitigation Plan to address its violation of CIP-004-1 R2 was submitted to WECC on March 19, 2010. The Mitigation Plan was accepted by WECC on November 19, 2010 and approved by NERC on December 15, 2010. The Mitigation Plan for this violation is designated as MIT-08-3150 and was submitted as non-public information to FERC on December 17, 2010 in accordance with FERC orders. URE submitted a request for Mitigation Plan extension and revised Mitigation Plan revision to include additional time needed to complete training for contractors and service vendors with authorized access to CCAs.

URE's Mitigation Plan required URE to:

1. Create a new centralized cybersecurity training program;
2. Revise training program to include all criteria listed under R2.2; and
3. Ensure all employees with authorized access to CCAs complete cybersecurity training.

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

1. CIP security training program, PRA, training, and authorized access provisioning procedures;
2. NERC CIP training documentation (URE has updated its general access training to include all required elements specified in requirements R2.2.1 through R2.2.4); and

3. NERC CIP training dates (a spreadsheet listing URE's personnel with access to CCAs and their most recent dates of training).

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

WECC201002306 CIP-004-1 R4

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to WECC. WECC issued a notice of Mitigation Plan rejection and request for revised Mitigation Plan to address the full scope of the noncompliance as described in the Notice of Alleged Violation of CIP-004-1 R4. URE submitted its revised Mitigation Plan. WECC reviewed the revised Mitigation Plan and issued a notice of revised Mitigation Plan acceptance. The Mitigation Plan was accepted by WECC on December 8, 2011 and approved by NERC on January 10, 2012. The Mitigation Plan for this violation is designated as WECCMIT005627 and was submitted as non-public information to FERC on January 10, 2012 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Update its list of personnel with access to CCAs. All employees who were added to the list were properly authorized under CIP-004-1 and no changes to employee access were required;
2. Revoke access immediately upon discovery of the violation;
3. Update its access tracking database to include the employee's cyber access to a shared operator HMI password; and
4. Review its CIP-004-1 R4 plant procedure and implement necessary revisions.

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

1. An interconnected entity/URE agreement that mandates specific responsibilities including processes for access;
2. URE's access lists review procedure;
3. URE's cyber access quarterly review;
4. URE's facility procedures;
5. URE's cyber access form; and
6. URE's updated CCA access list.

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

WECC201002307 CIP-005-1 R1

URE submitted a Mitigation Plan addressing possible noncompliance with CIP-005-1 R1. URE submitted a revised Mitigation Plan and request for extension. The Mitigation Plan was accepted by WECC on September 15, 2011 and approved by NERC on October 19, 2011. The Mitigation Plan for this violation is designated as WECCMIT004329 and was submitted as non-public information to FERC on October 20, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to implement a separate remote access solution that has the controls required by CIP-005-1 R1.5, in place of the assets used in controlling access to the ESP.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted drawings, logs and a master list of Cyber Assets.

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

WECC201002308 CIP-006-2 R1

URE submitted two Mitigation Plans addressing the violation of CIP-006-2 R1. WECC issued a Notice of Mitigation Plan Rejection and Request for Revision. In the notice, WECC requested that URE submit a single Mitigation Plan addressing the full scope of noncompliance with CIP-006-2 R1. URE resubmitted a Mitigation Plan. The Mitigation Plan was accepted by WECC on December 15, 2011 and approved by NERC on January 10, 2012. The Mitigation Plan for this violation is designated as WECCMIT004330 and was submitted as non-public information to FERC on January 10, 2012 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Deploy and document measures to control physical access to a facility escape hatch;
2. Review and assess the other access points to the facility;
3. Deploy and document additional measures to control physical access to the facility's PSPs;
4. Review and assess the other PSPs of the project for several functions;
5. Deploy and document any additional measures to control physical access to the other PSPs of the facility;
6. Update the operational and procedural controls for managing and monitoring physical access to the PSPs of the facility;

7. Send out a targeted communication to all facility operators of the protocol/procedures for escorting visitors at the different PSPs at the site; and
8. Review system logs and confirm that there were no attempts to log on and no external devices introduced to any CCAs.

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

1. CIP-006 physical security plan document;
2. A facility reference diagram;
3. Facility PSP documentation; and
4. Revised facility CIP operation and PSP access control procedures.

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

WECC201002310 CIP-007-1 R1

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to WECC on March 21, 2012. The Mitigation Plan was accepted by WECC on April 19, 2012 and approved by NERC on May 9, 2012. The Mitigation Plan for this violation is designated as WECCMIT007030 and was submitted as non-public information to FERC on May 11, 2012 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Create a testing procedure that identifies the circumstances triggering a cybersecurity test;
2. Ensure that new Cyber Assets and all significant changes to existing Cyber Assets within the ESP do not affect existing cybersecurity controls; and
3. Create a testing template designed to test all applicable CIP device types and address test procedures to assess significant changes to these device types.

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

1. Revised CIP-007-R1 EMS security test procedure;
2. Test results template;
3. Revised CIP-007-R1 security test procedure;

4. Revised appendix of the CIP-007-R1 security test procedure; and
5. Test results template.

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

WECC201002311 CIP-007-1 R3

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to WECC on November 17, 2011. The Mitigation Plan was accepted by WECC on December 14, 2011 and approved by NERC on January 10, 2012. The Mitigation Plan for this violation is designated as WECCMIT004590 and was submitted as non-public information to FERC on January 10, 2012 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Install a certain program on all HMIs for anti-virus and malware protection;
2. Revise its anti-virus and malware update procedures;
3. Hardcode firewalls, routers and computer devices and require authentication for access; and
4. Revise, sign and implement new procedures to track certain program updates.

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

1. Revised CIP-003-2 R6 change control and configuration management form;
2. Revised CIP-007-2 facility procedures; and
3. Revised CIP-007-2 R3 tracking patch management procedure.

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

WECC201102539 PRC-005-1 R2

URE submitted to WECC a Mitigation Plan addressing noncompliance with PRC-005-1 R2. URE submitted to WECC a revised Mitigation Plan that included updated completion dates and removed one milestone. The Mitigation Plan was accepted by WECC on June 15, 2012 and approved by NERC on July 17, 2012. The Mitigation Plan for this violation is designated as WECCMIT006080 and was submitted as non-public information to FERC on July 19, 2012 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revise its maintenance practices to incorporate industry best practices for battery maintenance, in addition to adjusting maintenance intervals and clearly identifying specific tasks on maintenance reports;
2. Train battery maintenance crews;
3. Begin implementation of revised maintenance practices;
4. Test and maintain 100 percent of its batteries;
5. Identify all gaps between specific plant maintenance practices and URE's Program; and
6. Update the Program and associated maintenance procedures and perform additional maintenance if required.

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

1. Revised Program document;
2. Station battery and battery charger maintenance procedure;
3. Substation battery list with dates of last semi-annual battery inspection;
4. Generation battery list with dates of last semi-annual battery inspection;
5. Generation gap analysis;
6. Generation PT and CT inspection form;
7. Generation battery selection methodology; and
8. Generation PT and CT component list with dates of last inspection.

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

WECC201102537 PRC-008-0 R2

URE submitted to WECC a Mitigation Plan addressing noncompliance with PRC-008-0 R2. URE submitted to WECC a revised Mitigation Plan that included updated completion dates and removed one milestone. The Mitigation Plan was accepted by WECC on June 19, 2012 and approved by NERC on July 17, 2012. The Mitigation Plan for this violation is designated as WECCMIT006079 and was submitted as non-public information to FERC on July 19, 2012 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revise its maintenance practices to incorporate industry best practices for battery maintenance, in addition to adjusting maintenance intervals and clearly identifying specific tasks on maintenance reports;
2. Train battery maintenance crews;
3. Begin implementation of revised maintenance practices;
4. Test and maintain 100 percent of its batteries;
5. Identify all gaps in specific plant maintenance practices and URE's Program; and
6. Update the Program and associated maintenance procedures and perform additional maintenance if required.

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

1. Revised Program document;
2. Station battery and battery charger maintenance procedure;
3. Substation battery list with dates of last semi-annual battery inspection;
4. Generation battery list with dates of last semi-annual battery inspection;
5. Generation gap analysis;
6. Generation PT and CT inspection form;
7. Generation battery selection methodology; and
8. Generation PT and CT component list with dates of last inspection.

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

WECC201002373 VAR-002-1.1b R3

URE's Mitigation Plan to address its violation of VAR-002-1.1b R3 was submitted to WECC on December 30, 2010. The Mitigation Plan was accepted by WECC on January 18, 2011 and approved by NERC on February 28, 2011. The Mitigation Plan for this violation is designated as MIT-10-3336 and was submitted as non-public information to FERC on February 28, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to require all plant operations and management personnel at a specific facility to complete retraining on reporting and notice procedures as required by the Standard.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted a record of training completion.

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

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[19]

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,[20] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2012. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a two hundred seven thousand dollar ($207,000) 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 received self-reporting credit for the CIP-002-1 R3 , CIP-003-1 R1, CIP-007-1 R3 and VAR-002-1.1b violations, as discussed above;
2. URE did not receive self-reporting credit for the CIP-004-1 R2 and R4 violations because it self-reported during the Self-Certification period;
3. URE did not receive self-reporting credit for the PRC-005-1 R2 and PRC-008-0 R2 violations because it self-reported after the WECC audit team had already identified the violations;

[19] *See* 18 C.F.R. § 39.7(d)(4).
[20] *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).

4. WECC reviewed URE's internal compliance program (ICP) and considered it a mitigating factor in penalty determination;
5. URE was cooperative throughout the compliance enforcement process;
6. URE did not fail to complete any applicable compliance directives;
7. There was no evidence of any attempt by URE to conceal the violations;
8. There was no evidence that URE's violations were intentional; and
9. WECC considered as an aggravating factor some elements of URE's violation history.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred seven thousand dollars ($207,000) 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-002-1 R1 included as Attachment b:

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

c) Record documents for the violation of CIP-002-1 R3 included as Attachment c:

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

d) Record documents for the violation of CIP-003-1 R1 included as Attachment d:

   1. URE's Self-Report;
   2. URE's Mitigation Plan;
   3. URE's Certification of Mitigation Plan Completion; and
   4. WECC's Verification of Mitigation Plan Completion.

e) Record documents for the violation of CIP-004-1 R2 included as Attachment e:

   1. URE's Self-Report;
   2. URE's Mitigation Plan;
   3. URE's Certification of Mitigation Plan Completion; and
   4. WECC's Verification of Mitigation Plan Completion.

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

   1. URE's Self-Report;
   2. URE's Mitigation Plan;

3. URE's Certification of Mitigation Plan Completion; and
4. WECC's Verification of Mitigation Plan Completion.

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

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

h) Record documents for the violation of CIP-006-2 R1 included as Attachment h:

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

i) Record documents for the violation of CIP-007-1 R1 included as Attachment i:

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

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

1. URE's Self-Report;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion; and
4. WECC's Verification of Mitigation Plan Completion.

k) Record documents for the violation of PRC-005-1 R2 included as Attachment k:

1. URE's Self-Report;
2. URE's Mitigation Plan;

3. URE's Certification of Mitigation Plan Completion; and
4. WECC's Verification of Mitigation Plan Completion.

l) Record documents for the violation of PRC-008-0 R2 included as Attachment l:

1. URE's Self-Report;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion; and
4. WECC's Verification of Mitigation Plan Completion.

m) Record documents for the violation of VAR-002-1.1b R3 included as Attachment m:

1. URE's Self-Report;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion; and
4. WECC's Verification of Mitigation Plan Completion.

A Form of Notice Suitable for Publication[21]

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

[21] *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	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Meredith May Jolivert* Attorney North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile rebecca.michael@nerc.net meredith.jolivert@nerc.net
Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 713-9598 (801) 582-3918 – facsimile Mark@wecc.biz Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6885 (801) 883-6894 – facsimile CWhite@wecc.biz	Christopher Luras* Manager of Compliance 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 RArredondo@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/ Rebecca J. Michael

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

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Meredith May Jolivert
Attorney
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
rebecca.michael@nerc.net
meredith.jolivert@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments