PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

November 30, 2011

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. NP12-_-000

Dear Ms. Bose:

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

URE submitted a Self-Certification[3] addressing the following violations[4] of Reliability Standards:

1. CIP-004-1 Requirement (R) 2 for URE's failure to ensure that all URE personnel having authorized access to Critical Cyber Assets (CCAs), including contractors and service vendors, were trained within ninety calendar days of such authorization,

[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] WECC notified URE that WECC was initiating the CIP Self-Certification process. Although URE self-reported the violations, because URE self-reported during the Self-Certification submission period, the discovery method for each violation is classified as Self-Certification.

[4] 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.

URE's failure to annually train all of its personnel and contractors with such access, and URE's failure to provide cyber security training covering URE's policies, access controls, and procedures as developed for the CCAs covered by CIP-004;

2. CIP-004-1 R3 for URE's failure to conduct personnel risk assessments (PRAs) on all of its personnel or contractors within 30 days of the personnel or contractor gaining access to CCAs; and
3. CIP-004-1 R4 for URE's failure to revoke authorized access to CCAs within 24 hours for personnel terminated for cause and within seven calendar days for changes in personnel with or changes in access rights to CCAs, as well as URE's failure to maintain lists of contractors with authorized cyber or authorized unescorted physical access to CCAs.

URE submitted Self-Reports addressing the following violations of Reliability Standards:

1. CIP-005-1 R2 for URE's failure to use an access control model that denies access by default, URE's failure to enable only ports and services required for operations and for monitoring CAs within the Electronic Security Perimeter (ESP), and URE's failure to implement strong procedural or technical controls at ESP access points to ensure authenticity of the accessing party;
2. CIP-007-1 R2 for URE's failure to establish a process to ensure that only those ports and services required for normal and emergency operations are enabled. As a result, URE enabled ports and services not required for normal and emergency operations and did not disable other ports and services prior to production use; and
3. CIP-007-1 R4 for URE's failure to document and implement a process for the testing and installation of anti-virus and malware prevention signature updates.

During an on-site compliance audit (Audit), WECC identified the following violations of Reliability Standards:

1. CIP-002-1 R1 for URE's failure to state how URE specifically considered all generation resources that support the reliable operation of the bulk power system (BPS) in its risk-based assessment methodology (RBAM);
2. CIP-002-1 R2 for URE's failure to identify its Substation A as a Critical Asset (CA) using the blackstart capability/connectivity evaluation criteria outlined in its RBAM;
3. CIP-002-1 R3 for URE's failure to identify CAs (that either use a routable protocol to communicate outside the ESP or a routable protocol within a control center) as CCAs;
4. CIP-003-1 R1 for URE's failure to address the requirements of CIP-002 through CIP-009 in its first cyber security policy;
5. CIP-003-1 R4 for URE's failure to implement a program that identifies, classifies and protects information associated with CCAs;

6. CIP-005-1 R1 for URE's failure to afford the protective measures specified in CIP-007 R5 to its four access points to the ESPs;
7. CIP-005-1 R3 for URE's failure to implement an electronic or manual process for monitoring and logging access at access points to its ESP twenty-four hours a day, seven days a week;
8. CIP-005-1 R4 for URE's failure to include the discovery of all access points to the ESP in its 2009 cyber vulnerability assessment;
9. CIP-006-1 R2 for URE's failure to provide all of the protective measures afforded by CIP-004 R3, CIP-007 R2 and CIP-007 R6 to three Physical Security Perimeter (PSP) access control and monitoring devices (ACMs); and
10. CIP-007-1 R5 for URE's failure to review, at least annually, user accounts to verify that access privileges are in accordance with Standard CIP-003 R5 and Standard CIP-004 R4.

This Notice of Penalty is being filed with the Commission because WECC and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations of CIP-002-1 R1, R2 and R3, CIP-003-1 R1 and R4, CIP-004-1 R2, R3 and R4, CIP-005-1 R1, R2, R3 and R4, CIP-006-1 R2, and CIP-007-1 R2, R4 and R5. According to the Settlement Agreement, URE stipulates and agrees to the facts of the violations and has agreed to the assessed penalty of one hundred sixty thousand dollars ($160,000), 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 WECC201002090, WECC201002091, WECC201002092, WECC201002093, WECC201002094, WECC201002096, WECC201002097, WECC201002098, WECC201002099, WECC201002100, WECC201002101, WECC201002102, WECC201002073, WECC201002103, WECC201002104 and WECC201002105 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 entered into as of August 15, 2011 and executed on August 17, 2011, 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 (2007), 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 ($)
WECC	Unidentified Registered Entity	NOC-958	WECC201002090	CIP-002-1[5]	1	Lower[6]	160,000
			WECC201002091	CIP-002-1[7]	2	High[8]	
			WECC201002092	CIP-002-1[9]	3	High[10]	
			WECC201002093	CIP-003-1	1	Lower[11]	
			WECC201002094	CIP-003-1[12]	4	Medium	
			WECC201002096	CIP-004-1[13]	2	Lower[14]	

[5] The duration of the violation covered Version 1, Version 2 and Version 3 of this Standard. For consistency, Version 1 will be used throughout.
[6] When NERC filed Violation Risk Factors (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.
[7] *See supra* n. 6.
[8] When NERC filed VRFs it originally assigned CIP-002-1 R2 a "Lower" 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 "Lower" VRF for CIP-002-1 R2 was in effect from June 18, 2007 until January 27, 2009 when the "High" VRF became effective.
[9] The duration of the violation covered both Version 1 and Version 2 of this Standard. For consistency, Version 1 will be used throughout.
[10] 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.
[11] CIP-003-1 R1 has a "Medium" VRF; CIP-003-1 R1.1, R1.2 and R1.3 each have a "Lower" VRF. 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. WECC determined that this is a violation of CIP-003-1 R1.1 and therefore a "Lower" VRF is appropriate.
[12] *See supra* n. 6.
[13] *See supra* n. 6.
[14] 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.

			WECC201002097	CIP-004-1[15]	3	Medium[16]	
			WECC201002098	CIP-004-1[17]	4	Medium[18]	
			WECC201002099	CIP-005-1[19]	1	Medium[20]	
			WECC201002100	CIP-005-1[21]	2	Medium[22]	
			WECC201002101	CIP-005-1[23]	3	Medium	
			WECC201002102	CIP-005-1[24]	4	Medium[25]	
			WECC201002073	CIP-006-1[26]	2[27]	Medium	
			WECC201002103	CIP-007-1[28]	2	Medium	
			WECC201002104	CIP-007-1[29]	4	Medium[30]	

[15] *See supra* n. 6.
[16] CIP-004-1 R3 has a "Medium" VRF; CIP-004-1 R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 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 R3 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.
[17] *See supra* n. 6.
[18] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; CIP-004-1 R4.2 has a "Medium" VRF. 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. WECC determined that this is a violation of CIP-004-1 R4.2 and therefore a "Medium" VRF is appropriate.
[19] *See supra* n. 10.
[20] 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.
[21] *See supra* n. 10.
[22] CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" VRF; CIP-005-1 R2.5 and its sub-requirements and R2.6 each have a "Lower" VRF.
[23] *See supra* n. 10.
[24] *See supra* n. 10.
[25] CIP-005-1 R4 and R4.2 each have a "Medium" VRF; CIP-005-1 R4.1 has a "Lower" VRF.
[26] *See supra* n. 6.
[27] As part of the Audit, violation findings made with respect to CIP-006-1 R1.8 fall under the scope of CIP-006-2c R2; as part of CIP Version 2, CIP-006-1 R1.8 was updated and included in CIP-006-2 R2.2.
[28] *See supra* n. 10.
[29] *See supra* n. 10.
[30] When NERC filed VRFs it originally assigned CIP-007-1 R4 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 February 2, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-007-1 R4 was in effect from June 18, 2007 until February 2, 2009, when the "Medium" VRF became effective.

			WECC201002105	CIP-007-1[31]	5	Medium[32]	

WECC201002090 CIP-002-1 R1

The purpose of Reliability Standard CIP-002-1 provides in pertinent part:

> 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.…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.

CIP-002-1 R1 provides:

> R1. Critical Asset Identification Method — The Responsible Entity [33] 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.

[31] *See supra* n. 6.

[32] CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, R5.2.2, R5.3, R5.3.1 and R5.3.2 each have a "Lower" VRF; CIP-007-1 R5.1, R5.1.3, R5.2.1, R5.2.3 and R5.3.3 each have a "Medium" VRF. WECC determined that this is a violation of CIP-007-1 R5.1.3 and therefore a "Medium" VRF is appropriate.

[33] Within the text of the CIP Standards, "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.

> R1.2.4. 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.

[Footnote added.]

CIP-002-1 R1 has a "Lower" VRF.[34]

Prior to the Audit, URE submitted approximately sixty documents (*e.g.*, RBAM, current planning studies, blackstart procedures, contingency response procedures and one-line diagrams). During and prior to the Audit, WECC reviewed URE's documentation and determined URE's RBAM addressed each of the sub-requirements of this Standard with the exception of R1.2.3. WECC noted that URE declared it is a net importer of energy and that its generation is not critical to the BPS. As a result, WECC submitted a data request to URE and conducted interviews with URE personnel. During the interview, WECC asked URE personnel to provide URE's evaluation criteria for generation resources that support the reliable operation of the BPS.

URE's CIP subject matter experts (SMEs) stated they did not have additional information beyond what URE previously provided that identifies generation resources that support the reliable operations of the BPS. URE submitted information to elaborate that the RBAM must consider generation resources that support the reliable operation of the BPS. URE explained that its operating studies for importing power demonstrate that URE does not have specific generating resources that support the reliable operation of the BPS, other than those units

[34] At the time of these violations, no VSLs were in effect for CIP-002-1 – CIP-009-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

identified as generating resources that provide blackstart capability. URE further added that it drafted a clarifying memorandum explaining the manner in which URE's RBAM considers generation resources that support the reliable operation of the BPS, but URE did not change the RBAM document. WECC determined that URE had a violation of CIP-002-1 R1 because URE failed to state how it specifically considered all generation resources that support the reliable operation of the BPS in its RBAM.

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

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE relies on its generation to serve its load and is a net importer of energy. URE's operating studies for importing power demonstrate that URE does not have specific generating resources that support the reliable operation of the BPS, other than those units identified as generating resources that provide blackstart capability.

WECC201002091 CIP-002-1 R2

CIP-002-1 R2 provides: "Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary."

CIP-002-1 R2 has a "High" VRF.

During and prior to the Audit, WECC reviewed URE's lists of CAs. WECC interviewed URE personnel to gain a full understanding of URE's approach to applying its RBAM. WECC reviewed eight URE CA lists. WECC subsequently reviewed URE's RBAM in comparison to URE's identified CAs. WECC identified URE's substation A as a CA pursuant to URE's RBAM, which had been left off of URE's CA list despite URE's RBAM procedure calling for URE to include "230/115/69/21 kV Substations" on its asset list. WECC determined that URE had a violation of CIP-002-1 R2 because URE failed, in its annual application of its RBAM, to identify substation A as a CA using the blackstart capability/connectivity evaluation criteria outlined in the URE RBAM.

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

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because even though the substation was not on the CA list, URE protected the substation in the same manner as its other CA substations. Additionally, the classification of the substation at issue did not result in the identification of any new CCAs.

WECC201002092 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 inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, 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.

During and prior to the Audit, WECC discovered that URE determined it did not have CCAs at substations URE had deemed CAs. WECC reviewed URE's undated serial relay connection diagram and noted the diagram showed a router connected to a telecom network. WECC reviewed URE's documentation in order to understand URE's assessment of its routable protocol devices and serial-connected (but Internet Protocol (IP) accessible) relays. In interviews, URE SMEs discussed URE's routers as "pass through devices." WECC determined such routers are manufactured, configured and installed as IP-accessible units capable of forwarding IP traffic between devices of disparate physical connections (*e.g.*, Ethernet and serial). WECC further determined such routers function as IP-accessible terminal servers. The routers are layer 3 devices with active IP-enabled access ports connected to a URE telecom network. WECC confirmed this determination at URE's seven other substations.

WECC also determined URE operated four Energy Management System (EMS) network devices as access points to URE's system control center and backup control center. The four network devices are essential to the operation of the control center and backup control center.

Pursuant to URE's RBAM, URE designated the control center and backup control center as CAs. URE's routers use a routable protocol to communicate outside the ESP and the four EMS network devices use a routable protocol within a control center. None of these routers or network devices were identified as CCAs.

WECC determined that URE had a violation of CIP-002-1 R3 because URE failed to identify certain CAs (that used either a routable protocol to communicate outside the ESP or a routable protocol within a control center) as CCAs.

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

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because although URE did not identify the devices described above as CCAs, URE did provide other protections to the devices. For example, URE's routers are accessible via URE's fiber optic network, which URE monitors as part of its normal operations. With regard to the four network devices, URE had initially classified these devices as CCAs and afforded the devices the full protections of CIP-003 through CIP-009. URE subsequently reclassified these devices as ACMs. During the time of the violation, URE's protective measures for the network devices did not change, and despite not being identified as CCAs, WECC verified URE maintained the devices in accordance with CIP-003 through CIP-009.

WECC201002093 CIP-003-1 R1

The purpose of Reliability Standard CIP-003-1 provides in pertinent part: "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.

CIP-003-1 R1 has a "Lower" VRF.

During the Audit, URE submitted four crosswalk documents (documents mapping URE's cyber security policy to NERC Standards CIP-002 through CIP-009) to WECC. WECC determined URE's cyber security policy - Version 1 did not fully address each of the requirements of CIP-002 through CIP-009. The first version of the URE Cyber Security Policy included an overarching statement that URE would comply with the CIP standards instead of specifically and fully addressing each of the requirements of CIP-002 through CIP-009. URE's Version 2 through Version 4 crosswalk documents did fully address CIP-003-1 R1. WECC determined all versions of URE's cyber security policy represented URE management's commitment and ability to secure its CCAs, however, WECC determined URE did not address each of the requirements of CIP-002 through CIP-009 in its first cyber security policy.

WECC determined the duration of the violation to be from the date the Standard became 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 because URE's Version 1 policy demonstrated a high-level commitment to cyber security and URE's senior manager did conduct an annual review of URE's cyber security policy in 2009 and 2010.

WECC201002094 CIP-003-1 R4
CIP-003-1 R4 provides:

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

> R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

CIP-003-1 R4 has a "Medium" VRF.

During the Audit, URE provided a confidential information protection policy. WECC reviewed this policy document and URE's associated documents. URE conducted an annual review as required by R4.3, and during this review, URE documented instances where it did not implement its policy. URE created an action plan to improve its information protection program, but had not made progress on its action plan. WECC determined URE had documented a program to identify, classify and protect information associated with its CCAs pursuant to R4.1 and R4.2, and that URE conducted an annual assessment pursuant to R4.3 but did not demonstrate that it implemented its information protection program. WECC identified several instances where URE labeled CCA information in a manner other than that prescribed in URE's information protection program.

WECC determined that URE had a violation of CIP-003-1 R4 because URE failed to follow URE's information protection program for document classification, and URE did not implement its program to identify, classify and protect information associated with CCAs.

WECC determined the duration of the violation to be from the date the Standard became 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 because URE had a documented information protection program and URE took steps to protect such information. URE's failure in this case stems from a failure to fully and accurately implement its program by not labeling information in accordance with the designated labeling set forth in URE's information protection program. URE did protect its CCA information by labeling documentation "confidential" and placing distribution restrictions on information related to CCAs.

WECC201002096 CIP-004-1 R2

The purpose of Reliability Standard CIP-004-1 provides in pertinent part: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-004-1 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 "Lower" VRF.

URE conducted an internal review, discovered and self-reported a possible non-compliance with this Standard. URE stated that it had "established, maintained and documented an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCA),"[35] but that "several existing

[35] *See supra* n. 4.

employees and certain contractors ... did not undergo the training within ninety (90) calendar days of authorization or receive the annual training."

During and prior to the Audit, WECC reviewed URE's Self-Report, as well as the evidence URE submitted during the Audit. URE did not ensure that all URE personnel having such access to CCAs, including contractors and service vendors, were trained within ninety calendar days of such authorization. Further, URE did not maintain documentation that it conducted training for these individuals at least annually. Also, because these individuals did not undergo URE's cyber security training, these individuals did not receive training pursuant to R2.2 of the Standard. WECC determined between 5 percent and 10 percent of all URE personnel having access to CCAs, including contractors and service vendors, were not trained within ninety calendar days of such authorization.

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

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because the violation is limited to a small percentage of URE personnel and contractors that had existing authorized access and experience handling CCAs.

WECC201002097 CIP-004-1 R3
CIP-004-1 R3 provides:

> R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:
>
> > R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (*e.g.*, Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

> R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.
>
> R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

CIP-004-1 R3 has a "Medium" VRF.

URE conducted an internal review, discovered and self-reported that it had "identified certain instances in which [URE] lacks documentation to demonstrate that background checks were performed or updated in accordance with the standard."[36] According to the Self-Report, the employees involved are long-time URE personnel. URE further stated on the Self-Report "certain contractor personnel with authorized access to CCA were overlooked due to an administrative oversight and do not appear to have undergone a personnel risk assessment."

During the Audit, WECC reviewed URE's Self-Report, as well as the evidence URE submitted during the Audit. WECC found three URE personnel had not received PRAs after a seven-year renewal period. In addition, URE employees with access to ACMs had not received a PRA within thirty days of gaining access to the ACMs. As a result, WECC determined URE could not provide documentation demonstrating it conducted a PRA for personnel and contractors with authorized cyber or unescorted physical access to CCAs within 30 days of URE granting personnel or contractors such access. WECC determined there was a violation of CIP-004-1 R3 because URE failed to conduct PRAs on some of its personnel or contractors within 30 days of the personnel or contractor gaining access to CCAs.

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

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because the violation was limited to URE personnel and contractors that had existing access and experience handling CCAs.

[36] *See supra* n. 4.

WECC201002098 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.

URE conducted an internal review, discovered and self-reported a possible non-compliance with this Standard. URE stated that while it had "developed a list of personnel with authorized cyber or authorized unescorted physical access to CCA."[37] URE's compliance department's internal review revealed the following:

> Instances in which the list of personnel with authorized cyber or authorized unescorted physical access to CCA were not updated within seven calendar days, per R4.1. [URE] further discovered one instance in which [URE] terminated an employee for cause and did not remove cyber access within 24 hours.[38] Such review also discovered that access lists for contractors were not properly maintained.

During and prior to the Audit, WECC reviewed URE's Self-Report, as well as the evidence URE submitted during the Audit. WECC determined URE did not revoke access to CCAs within 24

[37] *See supra* n. 4.

[38] In its Mitigation Plan, URE noted that it located the documentation that demonstrated timely removal of the access for the terminated employee after it filed its Self-Report. The supervisor of the employee maintained this documentation, which highlighted the need to have a centralized location for the data.

hours for URE personnel terminated for cause and within seven calendar days for a change in URE personnel or change in access rights for personnel with access to CCAs.

WECC determined the duration of the violation to be from the date the Standard became 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 because there were physical and electronic controls, established in accordance with other CIP standards, which served as the primary barrier to unauthorized access to CCAs, in the absence of an access list. URE's violation is limited to individuals that URE had granted unescorted access rights to and is specific to maintenance of the access list, not the ability for these individuals to gain access.

WECC201002099 CIP-005-1 R1

The purpose 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.

During and prior to the Audit, WECC reviewed URE's documents on ESP management and URE's CCA inventory. Based on these documents, WECC determined URE identified a number of ESPs, each with a number of access points.

URE also provided a detailed diagram that identified networks and link ports, as well as described the four switches URE uses as access points and IP ranges and VLAN information related to the ESPs. WECC asked URE to demonstrate that it afforded the protective measures specified in CIP-003, CIP-004 R3, CIP-005 R2 and R3, CIP-006 R2 and R3, CIP-007 R1 and R3 through R9, CIP-008 and CIP-009 to its ESPs' ACMs. URE could not demonstrate it reviewed, at least annually, user accounts to verify access privileges are controlled in accordance with CIP-003 R5 and CIP-004 R4. CIP-007 R5.1.3 requires this annual access privilege verification review. Therefore, WECC determined URE did not afford the protective measures as specified in CIP-007 R5 to its ESPs' ACMs, in violation of the Standard.

WECC determined the duration of the violation to be from the date the Standard became 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 because URE did apply the protective measures specified in CIP-

003, CIP-004 R3, CIP-005 R2 and R3, CIP-006 R2 and R3, CIP-007 R1, R3, R4, R6, R7, R8 and R9, CIP-008 and CIP-009 to its ESPs' ACMs, and the violation was limited to the failure to review user accounts annually.

WECC201002100 CIP-005-1 R2

CIP-005-1 R2 provides:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
>
> R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
>
> R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
>
> R2.5. The required documentation shall, at least, identify and describe:
>
> R2.5.1. The processes for access request and authorization.
>
> R2.5.2. The authentication methods.
>
> R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

> R2.5.4. The controls used to secure dial-up accessible connections.
>
> R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

CIP-005-1 R2 has a "Medium" VRF.

URE conducted an internal review, and, as a result, URE submitted a Self-Report stating that, upon reviewing a vulnerability assessment, "it was determined that there were additional ports and services available at the Critical Cyber Assets(s)..." Specifically, URE stated on the Self-Report "there is network to network and IP to IP communication that does not specifically have any ports and services filtered at the Electronic Security Perimeter…."

During the Audit, WECC reviewed URE's Self-Report, as well as the evidence URE submitted during the Audit. Based on URE's self-reported information and URE's traffic filtering rules (on the access points), WECC determined URE did not ensure that it restricted access through URE's ESPs. URE provided drawings and narrative discussions of its ESPs. URE also provided copies of its access control lists deployed at the ESP. URE's final statement in its access control lists was a "deny ip any any" statement. WECC determined such a statement results in the denial of all traffic not permitted by a previous statement. CIP-005-1 R2.1 requires URE to deny access by default, such that explicit access permissions are specified. WECC determined that URE's access control policy allowed a significant amount of access by default rather than denying access by default.

WECC also reviewed the nature of interactive access permitted through URE's ESP boundaries, as well as the complete context of the controls around that access. Due to the permissive nature of the configured access lists on URE's ESP access points, URE did not demonstrate the full extent of external, interactive access available. Based on a review of the configuration files relevant to a security tool that can be configured to limit access based on the source address of incoming connections, WECC determined a significant number of devices outside URE's ESPs are allowed to initiate interactive access to a variety of services within the ESPs.

WECC determined that URE had a violation of CIP-005-1 R2 because IP filters are the only control deployed at the ESP boundary relative to external interactive access into the ESP. Since this control cannot determine the identity of the individual initiating the access, and since such access can be initiated from a variety of devices located at a variety of different locations, WECC determined that URE's controls for external interactive were not strong. WECC

determined that URE's access control policy allowed a significant amount of access by default rather than denying access by default. Finally, WECC also determined URE enabled ports and services not used for normal operations.

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

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE has an intrusion detection system in place that monitors for possible cyber security issues and alerts appropriate URE personnel when it detects any potential concerns. Further, URE's EMS application limited access to only specified users by user name and password. Additionally, URE implemented procedural and technical controls to help ensure only authorized users gained access to URE's CCAs. At the end of URE's access control rule set, URE used the "Deny IP any any log" command, which closed URE's systems to any IP address not otherwise specified as authorized.

WECC201002101 CIP-005-1 R3
CIP-005-1 R3 provides:

> R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.
>
> > R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.
> >
> > R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

CIP-005-1 R3 has a "Medium" VRF.

During the Audit WECC reviewed URE's electronic access control document and conducted an interview with URE SMEs. URE used a third-party service to monitor the intrusion detection

system installed within URE's ESP. URE uses a commercial security information management platform to collect security logs. WECC requested a sample of log data for a 24-hour period. URE provided the log as requested, however the log showed a time period wherein URE did not log all access to the ESP. As a result of this discrepancy, WECC conducted an interview with URE SMEs. In this interview, URE SMEs confirmed that URE did not log all approved access at access points to the ESPs twenty-four hours a day, seven days a week. As a result, WECC determined URE had a violation of CIP-005-1 R3 for URE's failure to implement an electronic or manual process for monitoring and logging access at access points to its ESPs twenty-four hours a day, seven days a week.

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

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE uses an intrusion detection system that detects and alerts for attempts at (or actual) unauthorized access. The alerts appropriately notify URE's designated response personnel. Finally, where URE collected logs, URE monitored and reviewed such logs.

WECC201002102 CIP-005-1 R4
CIP-005-1 R4 provides:

> R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> > R4.1. A document identifying the vulnerability assessment process;
> >
> > R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
> >
> > R4.3. The discovery of all access points to the Electronic Security Perimeter;
> >
> > R4.4. A review of controls for default accounts, passwords, and network management community strings; and,
> >
> > R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-005-1 R4 has a "Medium" VRF.

During and prior to the Audit, URE provided documentation demonstrating it conducted at least two cyber vulnerability assessments. WECC determined URE's first vulnerability assessment did not include sufficient steps to discover all access points to URE's ESP. WECC reviewed URE's document which referenced discovery of access points as follows, "[d]uring the course of the pre-assessment, a meeting was held to identify the access points that makeup the [Electronic Security Perimeter]."

URE did not provide WECC additional information or documentation related to discovering access points to its ESPs. URE SMEs were unable to describe any additional activities related to CIP-005-1 R4.2. WECC determined URE's "pre-assessment" meeting described above was not a sufficient cyber vulnerability assessment that included an assessment of the discovery of all access points to URE's ESPs. WECC determined URE's second cyber vulnerability assessment sufficiently demonstrated the elements of this Standard. WECC determined that URE had a violation of CIP-005-1 R4 because URE did not include the discovery of all access points to the ESP in its first cyber vulnerability assessment.

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

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE's cyber vulnerability assessment did include four of the five components within this Standard, and URE's SMEs conducted a tabletop discussion of known access points. In addition, WECC's SMEs determined that due to the design and location of URE's ESP, it is unlikely that unknown access points exist.

WECC201002073 CIP-006-1 R2

The purpose of Reliability Standard CIP-006-1 provides in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R2 provides:[39]

[39] CIP-006-2 R2 provides:

> R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
>
> R2.1. Be protected from unauthorized physical access.

> R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> > R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
> >
> > R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
> >
> > R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
> >
> > R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

CIP-006-1 R2 has a "Medium" VRF.

During the Audit, WECC determined URE's PSP ACMs are comprised of three workstations that host URE's PSP physical access control program client. These devices reside on URE's corporate network. The PSP physical access control program utilizes a server that resides on a firewalled segment of URE's corporate network. With respect to the three host workstations, WECC determined URE utilizes a central location service to authenticate users on each host workstation. As such, all individuals are capable of logging on to the host workstations.

WECC determined that URE had a violation of CIP-006-1 R2 because URE must provide protective measures to the host workstations. URE did not demonstrate that it performed a PRA for all personnel with corporate network access. Therefore, URE did not apply the protective measures of CIP-004 R3 to the host workstations. WECC further determined URE did not restrict ports and services on the host workstations, thus URE did not apply the protective

---

R2.2. Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.

measures of CIP-007 R2 to the host workstations. Finally, WECC determined that URE did not monitor security status on the host workstations, and therefore did not apply the protective measures of CIP-007 R6 to the host workstations. Accordingly, WECC determined that URE had a violation of CIP-006-1 R2.[40]

WECC determined the duration of the violation to be from the date the Standard became 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 because URE's strong physical security controls, dictated by external regulations, significantly reduce the attack vector on such devices. URE applies the security measures specified in CIP-003; CIP-005 R2 and R3; CIP-006 R4 and R5; CIP-008; and CIP-009 to the devices.

WECC2010020103 CIP-007-1 R2

The purpose 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 R2 provides:

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

[40] As part of the Audit, violation findings made with respect to CIP-006-1 R1.8 fall under the scope of CIP-006-2c R2; as part of CIP Version 2, CIP-006-1 R1.8 was updated and included in CIP-006-2 R2.2.

> compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R2 has a "Medium" VRF.

URE conducted an internal review. URE submitted a Self-Report stating that "it was determined that some of the previously documented ports and services were not necessary for normal and emergency operations." Specifically, URE stated on the Self-Report that "URE conducted a reconciliation of required ports for operations and management by URE against the actual ports and services open." Finally, URE clarified in the Self-Report that six ports and services discovered were not necessary

During and prior to the Audit, WECC reviewed URE's Self-Report, as well as the evidence URE submitted during the Audit. WECC conducted an interview with URE SMEs. The URE SMEs stated URE had relied on vendor documentation regarding required ports and services, but determined URE should conduct an in-house review. The URE SMEs stated that during the in-house review, URE security staff identified ports that URE operations staff had been using that presented a security risk. The URE SMEs stated URE security staff discovered enabled ports that were not necessary, and URE operations staff determined the enabled ports were convenient, but not necessary for normal or emergency operations.

During the Audit, WECC determined URE relied on its EMS manufacturer's default port and service specifications to ensure it only enabled the appropriate ports and services. WECC determined such reliance is not sufficient to serve as a process to identify those ports and services necessary for normal and emergency operations; WECC further determined the EMS manufacturer specifications cannot be related to all CAs within URE's ESP. Therefore, WECC determined the scope of URE's noncompliance expanded beyond that which URE self-reported.

WECC determined URE did not assess the functional nature of the ports and services as defined by the EMS manufacturer to determine if a port and service must be enabled to ensure operability of the CAs within the ESP. In short, WECC determined URE did not establish a process to ensure that only those ports and services required for normal and emergency operations are enabled. WECC determined URE's own cyber vulnerability assessment, a functional and security analysis, demonstrated that certain ports and services were not needed for normal or emergency operations (the cyber vulnerability assessment led to URE's Self-Report). WECC determined URE did not establish, document and implement a process to ensure that only those ports and services needed for normal and emergency operations are enabled. WECC determined URE did not provide documentation of the status of each port and service for each CA within the ESP and enabled ports and services not required for normal and emergency operations. Similarly, WECC determined URE did not disable other ports and

services, including those used for testing purposes, prior to production use of all CAs inside the ESP.

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

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE has an established intrusion detection system and a program which evaluates traffic and generates alerts as necessary.

WECC201002104 CIP-007-1 R4
CIP-007-1 R4 provides:

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

CIP-007-1 R4 has a "Medium" VRF.

URE conducted an internal review and submitted a Self-Report stating that "signature files for the … antivirus protection application are downloaded from the vendor site and distributed daily to the EMS development and production environments." Further, URE stated "that testing of the signatures files on a server outside [the ESP] is required prior to installation of the signature files on servers inside [the ESP]."[41]

[41] In the context of the Settlement Agreement, WECC and URE agreed to expand the scope of the violation to include a late-filed Technical Feasibility Exceptions (TFE) associated with the same standard and requirement. Specifically, URE had belatedly submitted a CIP-007-2 R4 TFE for new equipment placed into service, 30 days late. WECC reviewed and approved URE's TFE.

During the Audit, WECC reviewed URE's Self-Report, as well as the evidence URE submitted during the Audit, and conducted an interview with URE SMEs. URE historically relied on its anti-virus application to test signature files, but after attending workshops and taking part in CIP-related discussions, URE SMEs determined URE had to test the signatures files itself. The URE SMEs stated URE established an internal testing process after coming to the conclusion it reached prior to its Self-Report. Following the interview, WECC submitted a data request to verify that URE documented and implemented a process related to updating anti-virus and malware prevention signatures. WECC specifically requested that URE demonstrate its historical (prior to the Self-Report) process. URE provided the process document. WECC determined that URE had a violation of CIP-007-1 R4 because URE's document was not a process for the updating of anti-virus and malware prevention signatures, did not address testing and installing the signatures nor did it address malware prevention signatures, and therefore did not document such a process.

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

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE has redundant servers and a process in place wherein a failure of a primary server would start a redundant server. Thus, if a corrupt signature file rendered a primary server unstable or unavailable, URE's operations may be able to rely on a backup server.

WECC201002105 CIP-007-1 R5
CIP-007-1 R5 provides:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> > R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
> >
> > > R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

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

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

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

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

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

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

CIP-007-1 R5 has a "Medium" VRF.

During and prior to the Audit, WECC reviewed the evidence URE submitted as part of its pre-audit evidence submission. Based on the evidence provided, WECC could not determine if URE reviewed user accounts to verify access privileges are in accordance with CIP-003 R5 and CIP-004 R4. As a result, WECC conducted interviews and submitted multiple data requests. URE provided multiple documents to WECC, including evidence of eight quarterly reviews and a document listing user accounts, the groups to which the specified users belong, and user account privileges. URE did not provide evidence that it reviewed, on at least an annual basis, user account privileges for all CAs within URE's ESPs. URE provided evidence it reviewed user accounts associated with CCAs, but not non-critical CAs. As a result, WECC determined URE had a violation of CIP-007-1 R5 for failing to review user accounts to verify access privileges in accordance with CIP-004 R4 on CAs within the ESP.

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

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because although URE could not demonstrate that it conducted reviews on non-critical CAs, URE provided evidence demonstrating that it performed a majority of annual reviews of user accounts on CCAs.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred sixty thousand dollars ($160,000) for the referenced violations. In reaching this determination, WECC considered the following mitigating factors: URE self-reported the CIP-005-1 R2, CIP-007-1 R2 and the CIP-007-1 R4 violations; and URE had an internal compliance program (ICP) in place at the time of the violations. WECC also considered the entity's violation history in determining the penalty amount.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred sixty thousand dollars ($160,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plan[42]

WECC201002090 CIP-002-1 R1
URE's Mitigation Plan to address its violation of CIP-002-1 R1 was submitted to WECC on October 5, 2010 with a proposed completion date of October 22, 2010. The Mitigation Plan was accepted by WECC on March 11, 2011 and approved by NERC on April 28, 2011. The Mitigation Plan for this violation submitted as non-public information to FERC on May 2, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to add evaluation criteria for generating facilities to the RBAM of URE's operating procedures per CIP-002 R1.2.3. Evaluation criteria for generation resources that support the reliable operation of the BPS will be those URE generation facilities, either a single generating unit or a group of generating units at a single plant, that exceed the Most Severe Single Contingency (MSSC) of the Reserve Sharing Group, of which the URE BA was a participant.

URE certified on October 6, 2010 that the above Mitigation Plan requirements were completed on October 6, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Updated response procedure.

On March 29, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on October 6, 2010 and that URE had mitigated the violation of CIP-002-1 R1.

WECC201002091 CIP-002-1 R2
URE's Mitigation Plan to address its violation of CIP-002-1 R2 was submitted to WECC on October 5, 2010 with a proposed completion date of October 22, 2010. The Mitigation Plan was accepted by WECC on March 11, 2011 and approved by NERC on April 28, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on May 2, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to modify its operating procedure as follows:

1. Substation A was added under the "District Assets, Substations" section;
2. An "X" was placed in the "Facilities required for transmission supply/continuity" column making Substation A a CA; and

[42] *See* 18 C.F.R § 39.7(d)(7).

3. Additionally, Substation A was added to "Critical Asset List" under "Internal Transmission Substations."

URE certified on October 6, 2010 that the above Mitigation Plan requirements were completed on October 6, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Updated operating procedure.

On March 29, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on October 6, 2010 and that URE had mitigated the violation of CIP-002-1 R2.

WECC201002092 CIP-002-1 R3

URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to WECC on September 3, 2010 with a proposed completion date of September 3, 2010.[43] The Mitigation Plan was accepted by WECC on March 31, 2011 and approved by NERC on May 9, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on May 9, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Disconnect and remove URE's routers from the system; and
2. Classify the identified EMS network devices as both ACMs and as CCAs.

URE certified on September 3, 2010 that the above Mitigation Plan requirements were completed on September 3, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. A spreadsheet documenting URE's removal of the routers from its system.

On April 15, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on September 3, 2010 and that URE had mitigated the violation of CIP-002-1 R3.

WECC201002093 CIP-003-1 R1

URE's Mitigation Plan to address its violation of CIP-003-1 R1 was submitted to WECC on December 2, 2010 stating it had been completed on June 29, 2009. The Mitigation Plan was accepted by WECC on March 8, 2011 and approved by NERC on April 11, 2011. The Mitigation

[43] On October 5, 2010, URE re-submitted its Mitigation Plan using the Dynamic Forms feature on the WECC Compliance Web Portal.

Plan for this violation was submitted as non-public information to FERC on June 22, 2011 in accordance with FERC orders.

URE's Mitigation Plan stated that URE had staff attend a CIP user group meeting where they learned more about what policy components WECC auditors expected to see in an entity's CIP cyber security policy congruent to CIP-003 R1. URE staff took this new information and used it to revise its policy. The revised policy provides all of the requirements set forth in CIP-003 R1. Each of the CIP standards and requirements are listed as policy statements. This specifies URE management is committed to URE's ability to secure its CCAs.

URE certified on January 13, 2011 that the above Mitigation Plan requirements were completed on June 29, 2009. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. URE's version 2 of its cyber security policy.

On March 29, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on June 29, 2009 and that URE had mitigated the violation of CIP-003-1 R1.

WECC201002094 CIP-003-1 R4

URE's Mitigation Plan to address its violation of CIP-003-1 R4 was submitted to WECC on February 4, 2011 stating it had been completed on February 2, 2011.[44] The Mitigation Plan was accepted by WECC on March 11, 2011 and approved by NERC on April 11, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on April 12, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review its administrative policy and revise the policy to include and allow for the markings that are substantially similar to examples included in the policy to align the policy with URE's practices and ensure that its documents are labeled in accordance with its IPP; and
2. Reinforce the use of labeling on all documents and changes to the policy as a part of the annual CIP training for URE personnel with authorized unescorted physical access and authorized cyber access to CCAs.

[44] On October 14, 2010, URE submitted a Mitigation Plan to address this violation. The Mitigation Plan included an expected completion date of June 15, 2010. URE stated the cause of the violation stemmed from a failure to annually review its information protection program. WECC rejected the Mitigation Plan due to administrative error. On February 4, 2011, URE submitted a revised Mitigation Plan.

URE certified on February 4, 2011 that the above Mitigation Plan requirements were completed on February 2, 2011. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. URE's updated administrative policy.

On April 26, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on February 2, 2011 and that URE had mitigated the violation of CIP-003-1 R4.

WECC201002096 CIP-004-1 R2
WECC201002097 CIP-004-1 R3
WECC201002098 CIP-004-1 R4

URE's Mitigation Plan to address its violation of CIP-004-1 R2, R3 and R4 was submitted to WECC on February 26, 2010 with a proposed completion date of October 30, 2010. The Mitigation Plan was accepted by WECC on October 27, 2010 and approved by NERC on November 19, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on November 22, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to correct deficiencies inherent in the old manual diversified processes to maintain and retrieve documentation associated with meeting CIP-004-1 by:

1. Removed unescorted physical access for all employees and contractors lacking clear documentation that they had met training requirements, seven year background checks, or PRAs;
2. Centralized all records and responsibilities into one department;
3. Scaled back the number of employees with CCA access by 50% and an alternative to only include personnel that actually have access to the CCA areas;
4. Developed, tested, and qualified an automated compliance tool that can record, organize and quickly retrieve the required documentation; the tool contains work flow features to prevent employees or contractors from receiving unescorted physical or cyber access without proper training or PRAs being performed. It records all dates, times and authorizations as they occur and provides alerts and warnings when a time requirement in the Standard is approaching; and
5. Implemented the automated compliance tool replacing the manual process and trained all supervisors and personnel that have compliance roles with CIP-004-1 on the tool, its capabilities and documentation processes.

URE certified on October 29, 2010 that the above Mitigation Plan requirements were completed on October 29, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Evidence demonstrating URE developed the automated compliance tool and implemented the tool (as well as evidence related to 1-3, above).

On April 26, 2011, after reviewing URE's submitted evidence, WECC verified that URE mitigated the violation of CIP-004-1 R2 and R3. On May 26, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on October 29, 2010 and that URE had mitigated the violation of CIP-004-1 R4.

WECC201002099 CIP-005-1 R1

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was submitted to WECC on September 28, 2010 stating it had been completed on September 17, 2010.[45] The Mitigation Plan was accepted by WECC on March 16, 2011 and approved by NERC on April 28, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on May 2, 2011 in accordance with FERC orders.

URE's Mitigation Plan stated that for devices used in the access control and monitoring of the ESPs, URE applied the protective controls referenced in R1.5 for two new firewalls.

URE certified on March 14, 2011 that the above Mitigation Plan requirements were completed on December 14, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Annual user access review form; and
2. URE's list of users with access to all Cyber Assets.

On June 2, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on December 14, 2010 and that URE had mitigated the violation of CIP-005-1 R1.

[45] URE submitted a revised form on March 14, 2011 stating the mitigation activities for CIP-005-1 R1 were completed on December 14, 2010 to replace the September 17, 2010 Mitigation Plan that listed multiple CIP-005 requirements.

WECC201002100 CIP-005-1 R2

URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to WECC on September 3, 2010 stating it would be completed on September 17, 2010.[46] The Mitigation Plan was accepted by WECC on April 12, 2011 and approved by NERC on May 9, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on May 9, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Move the ESPs behind the existing firewall service modules at the control center and the backup control center making the firewall service modules the access points to the EMS ESPs;
2. Remove unnecessary network statements from each of the access lists;
3. Identify source host, destination host, destination ports and services for all communication into the ESP(s) where such restricted access is not already defined;
4. Modify the access control lists with the necessary source host, destination host, destination ports and services communications; and
5. Test and implement the updated restricted ports and services access control lists for the ESP.

URE certified on March 14, 2011 that the above Mitigation Plan requirements were completed on September 17, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Document 1; and
2. Document 2, both demonstrating how URE defined and restricted its ESPs.

On August 15, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on September 17, 2010 and that URE that it had mitigated the violation of CIP-005-1 R2.

WECC201002101 CIP-005-1 R3

URE's Mitigation Plan to address its violation of CIP-005-1 R3 was submitted to WECC on September 28, 2010 stating it had been completed on September 17, 2010. The Mitigation Plan was accepted by WECC on March 31, 2011 and approved by NERC on May 9, 2011. The

[46] On August 20, 2010, URE submitted a Mitigation Plan to address its self-reported violation. Before WECC reviewed this plan, on September 3, 2010, URE submitted a revised Mitigation Plan to address its noncompliance with CIP-005-2 R2.2.

Mitigation Plan for this violation was submitted as non-public information to FERC on May 9, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Implement a process for monitoring and logging access at the access points to the ESP through the use of a security information and event management (SIEM) application. All the access points to the ESP were configured to send logging information to the SIEM;
2. Developed monitoring and alerting functions generated by the SIEM which logs authorized access as well;
3. The access points define acceptable and approved traffic as well as not acceptable and unapproved traffic configured on the access points. This information was used to create correlation rules on the SIEM to further inspect traffic in the ESP which URE's information security office uses to create custom reports and alerts on the SIEM based on entries which are automatically sent daily to the URE EMS operations staff for review; and
4. The SIEM configuration is used in conjunction as a separate layer of defense with the intrusion detection system already in place at URE which are monitored twenty-four hours a day, seven days a week by a third party which alerts URE information security staff.

URE certified on March 14, 2011 that the above Mitigation Plan requirements were completed on September 17, 2010.[47] As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Logging reports for both permitted and denied access at all access points to the ESPs; and
2. Access control lists for the access points to the ESPs.

On June 2, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on September 17, 2010 and that URE had mitigated the violation of CIP-005-1 R3.

[47] URE submitted a revised Certification to replace the form submitted on September 17, 2010 which listed multiple CIP-005 requirements.

WECC201002102 CIP-005-1 R4

URE's Mitigation Plan to address its violation of CIP-005-1 R4 was submitted to WECC on October 14, 2010 stating it had been completed on May 28, 2010. The Mitigation Plan was accepted by WECC on March 29, 2011 and approved by NERC on April 11, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 22, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to perform the specific functions required by CIP-005 R4, including a process for discovery of all access points to the ESP. These processes were also documented as part of the cyber vulnerability assessment methodology employed by URE.

URE certified on January 13, 2011 that the above Mitigation Plan requirements were completed on May 29, 2010. URE's evidence of completion, which was URE's second cyber vulnerability assessment, was reviewed by WECC while on-site during the Audit.

On March 29, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on May 29, 2011 and that URE had mitigated the violation of CIP-005-1 R4.

WECC201002073 CIP-006-1 R2

URE's Mitigation Plan to address its violation of CIP-006-1 R2 was submitted to WECC on October 8, 2010 with a proposed completion date of December 20, 2010.[48] The Mitigation Plan was accepted by WECC on March 11, 2011 and approved by NERC on April 11, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on April 12, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Deploy the central location authentication service group policy object to limit the users that could log on to the physical access control system clients to only the authorized domain global group and domain administrators;
2. Remove Internet access from all workstations using a content filtering tool. Additionally, remove all unnecessary applications from the main station;
3. Disable the removable media ports of the three workstations;
4. Activate the forced door alarm on the main station door;

[48] On December 15, 2010, URE submitted a Mitigation Plan extension request form and revised Mitigation Plan. This revised Mitigation Plan included an expected completion date of January 31, 2011.

5. Install a CPU security cabinet in the main station machine to store the CPU, keyboard and mouse and issue controlled keys to security operations authorized staff who require access to the workstation;
6. In addition to the reader already on the main station door, install a PIN device requiring multifactor access to the door by each authorized person; and
7. Deploy technical controls on the workstations to require multi-factor authentication at the client for authentication.

URE certified on January 28, 2011[49] that the above Mitigation Plan requirements were completed on January 27, 2011. As evidence of completion of its Mitigation Plan, URE submitted the following which correspond to the mitigation activities listed above:

1. URE response to a data request and work order "tickets" used to track progress of an active directory group policy object to limit the users that could log on to the physical access control system clients;
2. Ticket #84075;
3. Ticket #84048;
4. Ticket # 84284;
5. Ticket #84274 and #84309; and
6. Narrative from URE summarizing actions taken and mapping evidence to the steps taken.

On May 6, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on January 27, 2011 and that URE had mitigated the violation of CIP-006-1 R2.

WECC201002103 CIP-007-1 R2

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to WECC on August 20, 2010 stating it had been completed on August 11, 2010. The Mitigation Plan was accepted by WECC on March 31, 2011 and approved by NERC on May 9, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on May 9, 2011 in accordance with FERC orders.

URE's Mitigation Plan stated URE's EMS support staff identified six ports as unnecessary for the operational functionality of the EMS environment. As such, URE EMS support staff removed or disabled the availability of these ports on all CCA and CA devices within the ESP. The removal of the identified ports was validated by performing a post-change port scan of all the devices within the ESP.

[49] The Settlement Agreement incorrectly lists the Certification date as January 31, 2011.

URE certified on August 26, 2010 that the above Mitigation Plan requirements were completed on August 11, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Evidence indexed per the above required actions and evidence a review was done to confirm the ports in scope are no longer active.

On April 20, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on August 11, 2010 and that URE had mitigated the violation of CIP-007-1 R2.

WECC201002104 CIP-007-1 R4

URE's Mitigation Plan to address its violation of CIP-007-1 R4 was submitted to WECC on August 13, 2010 stating it had been completed on August 12, 2010. The Mitigation Plan was accepted by WECC on March 4, 2011 and approved by NERC on March 25, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on March 25, 2011 in accordance with FERC orders.

URE's Mitigation Plan states URE has implemented an automated process to accomplish the testing of the daily signature files acquired from the anti-virus application. The application pushes out a new set of signature files each day to its website. URE will download this file set each day and immediately install on a test server outside of the ESP, followed by a demand scan utilizing the new signature file. Health monitoring of this server will continuously monitor for suspicious symptoms which could indicate a possible corrupt or compromised signature file. Upon successful completion of the monitoring period, the new signature files will be moved into the verified signature file repository for distribution to the servers inside the ESP. If the signature file test fails, then a log message is issued and email notification sent to the EMS support staff.

URE certified on August 26, 2010 that the above Mitigation Plan requirements were completed on August 12, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. The anti-virus application file signature file test;
2. Anti-virus and malware prevention management procedure;
3. Evidence of a meeting scheduled for URE SMEs to discuss CIP-005 and CIP-007 compliance; and
4. Evidence of testing to ensure anti-virus and anti-malware were receiving updates.

On April 12, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on August 12, 2010 and that URE had mitigated the violation of CIP-007-1 R4.

WECC201002105 CIP-007-1 R5

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to WECC on October 14, 2010 with a proposed completion date of December 20, 2010. The Mitigation Plan was accepted by WECC on March 30, 2011 and approved by NERC on March 25, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on March 25, 2011 in accordance with FERC orders.

URE's Mitigation Plan stated that URE has several separate lists containing pieces of information necessary for complying with this requirement. URE consolidated the existing multiple URE lists of user accounts and access privileges to include a single list of all CAs within the ESP into a single procedure. The new list includes the documentation and substantiation of the quarterly and annual review, as applicable per CIP-004 and CIP-007.

URE certified on December 20, 2010 that the above Mitigation Plan requirements were completed on December 14, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. CIP-007 R5 procedure document; and
2. Annual user access review form.

On April 12, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on December 14, 2011 and that URE that it had mitigated the violation of CIP-007-1 R5.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[50]

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,[51] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation

[50] *See* 18 C.F.R. § 39.7(d)(4).
[51] *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).

on October 11, 2011. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred sixty thousand dollar ($160,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. WECC considered URE's violation history;
2. URE self-reported the CIP-005-1 R2, CIP-007-1 R2 and CIP-007-1 R4 violations;
3. WECC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which WECC considered a mitigating factor as discussed above;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred sixty thousand dollars ($160,000) 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 executed August 15, 2011, included as Attachment a;

b) Record documents for 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;
4. WECC's Verification of Mitigation Plan Completion for CIP-002-1 R1 and R2;

c) Record documents for CIP-002-1 R2, included as Attachment c:

1. URE's Source Document;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion for CIP-002-1 R1 and R2, see Attachment b-4;

d) Record documents for CIP-002-1 R3, included as Attachment d:

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

e) Record documents for CIP-003-1 R1, included as Attachment e:

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

f) Record documents for CIP-003-1 R4, included as Attachment f:

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

g) Record documents for CIP-004-1 R2, R3 and R4, included as Attachment g:

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

3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion for CIP-004-1 R2 and R3;
5. WECC's Verification of Mitigation Plan Completion for CIP-004-1 R4;

h) Record documents for CIP-005-1 R1, included as Attachment h:

1. URE's Source Document;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion for CIP-005-1 R1 and R3;

i) Record documents for CIP-005-1 R2, included as Attachment i:

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

j) Record documents for CIP-005-1 R3, included as Attachment j:

1. URE's Source Document;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion for CIP-005-1 R1 and R3 , see Attachment h-4;

k) Record documents for CIP-005-1 R4, included as Attachment k:

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

l) Record documents for CIP-006-1 R2, included as Attachment l:

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

m) Record documents for CIP-007-1 R2, included as Attachment m:

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

n) Record documents for CIP-007-1 R4, included as Attachment n:

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

o) Record documents for CIP-007-1 R5, included as Attachment o:

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.

A Form of Notice Suitable for Publication[52]

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

[52] *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 30326-1001 (404) 446-2560 David N. Cook* Senior Vice President and General Counsel North American Electric Reliability Corporation 1120 G Street N.W., Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile david.cook@nerc.net	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net
Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 213-2673 (801) 582-3918 – facsimile Mark@wecc.biz	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
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	Sandy Mooy* Associate General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7658 (801) 883-6894 – facsimile SMooy@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 30326-1001
(404) 446-2560

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Sonia C. Mendonça
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments