PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

June 29, 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. NP11-_-000

Dear Ms. Bose:

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

This Notice of Penalty is being filed with the Commission because the Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of violations[3] of CIP-003-1, CIP-004-1, CIP-005-1, CIP-007-1 and CIP-009-1, further described below. According to the Settlement Agreement, URE agrees and stipulates to the facts of the violations and has agreed to the assessed penalty of one-hundred and forty-three thousand five-hundred dollars ($143,500), 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 WECC200901774, WECC200901773, WECC200901775, WECC201001856, WECC201001857, WECC201001858, WECC201001859, WECC201001860, WECC201001861, and

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).
[2] *See* 18 C.F.R § 39.7(c)(2).
[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

WECC201001862 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on February 14, 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	818	WECC200901774	CIP-005-1	3	Medium	143,500
			WECC200901773	CIP-007-1	5	Lower[4]	
			WECC200901775	CIP-007-1	6	Lower[5]	
			WECC201001856	CIP-003-1	1	Medium[6]	
			WECC201001857	CIP-004-1	2	Medium[7]	

[4] 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" Violation Risk Factor (VRF); R5.1, R5.1.3, R5.2.1 and R5.2.3 each have a "Medium" VRF. When NERC originally filed VRFs it originally assigned CIP-005-1 R5.1 and R5.3.3 "Lower" VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRFs and on August 20, 2009, the Commission approved the modified "Medium" VRFs. Therefore, the "Lower" VRFs for CIP-005-1 R5.1 and R5.3.3 were in effect from June 18, 2007 until August 20, 2009, when the "Medium" VRFs became effective.

[5] CIP-007-1 R6, R6.4 and R6.5 each have a "Lower" VRF and R6.1, R6.2 and R6.3 each have a "Medium" VRF.

[6] CIP-003-1 R1 has a "Medium" VRF; 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.

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

			WECC201001858	CIP-004-1	3	Medium[8]	
			WECC201001859	CIP-004-1	4	Lower[9]	
			WECC201001860	CIP-007-1	1	Medium[10]	
			WECC201001861	CIP-009-1	1	Medium	
			WECC201001862	CIP-009-1	2	Lower[11]	

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process.. URE self-reported violations of CIP-005-1 Requirement (R) 3, CIP-007-1 R5, and CIP-007-1 R6 to WECC for:

> (1) URE's failure to implement and document an electronic or manual process for monitoring and logging authorized user accounts, as well as URE's failure to detect and alert for attempts at or actual unauthorized accesses at URE's ESP in violation of CIP-005-1 R3;
>
> (2) URE's failure to establish, implement, and document technical and procedural controls that minimize the risk of unauthorized system access, as well as URE's failure to maintain historical audit trails of user account access for a minimum of ninety days, failure to minimize and manage the scope and acceptable use of administrator, shared, factory default, and other generic accounts, and failure to enforce complex passwords in violation of CIP-007-1 R5; and
>
> (3) URE failed to implement automated tools or organizational process controls to monitor system events that are related to cyber security on four HMI PCs in URE's Substation electronic security perimeter (ESP) and 43 workstations and servers in URE's energy management system (EMS) ESP in violation of CIP-007-1 R6.

WECC conducted an on-site CIP Spot Check at URE's facilities and identified violations of Reliability Standards CIP-003-1 R1, CIP-004-1 R2, R3, and R4, CIP-007-1 R1, CIP-009-1 R1 and CIP-009-1 R2 for:

---

[8] CIP-004-1 R3 has a "Medium" VRF; 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.

[9] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; 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.

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

[11] The Settlement Agreement incorrectly states that the CIP-009-1 R2 violation had a "Medium" VRF.

(1) URE's failure to document and implement a Cyber Security Policy addressing each of the requirements of CIP-002 through CIP-009 in violation of CIP-003-1 R1;

(2) URE's failure to ensure that all personnel, including contractors and service vendors, with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, were trained within ninety calendar days of such authorization; URE's failure to establish a Cyber Security Training Program ensuring employees, contractors, and vendors received training within 90 calendar days of gaining authorized unescorted physical access or cyber access to Critical Cyber Assets; URE's failure to include material specific to URE's personnel roles and responsibilities; and URE's failure to perform an annual review of its initial Cyber Security Training Program were violations of CIP-004-1 R2;

(3) URE's failure to conduct a Personnel Risk Assessment within thirty days of certain of URE's personnel being granted authorized cyber or authorized unescorted physical access to Critical Cyber Assets resulted in violation of CIP-004-1 R3;

(4) URE's failure to maintain and review a list of URE personnel who have electronic access to Critical Cyber Assets in violation of CIP-004-1 R4;

(5) URE's failure to document test results related to significant changes made to its servers in violation of CIP-007-1 R1;

(6) URE's failure to specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan in violation of CIP-009-1 R1; and

(7) URE's failure to exercise its recovery plan at least annually in violation of CIP-009-1 R2.

CIP-005-1 R3

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 R3 provides:

R3. Monitoring Electronic Access — The Responsible Entity[12] shall implement and document an electronic or manual process(es) for monitoring and logging

[12] Within the text of Standard CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

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.

WECC notified URE that WECC was initiating the semi-annual CIP self-certification process. URE discovered noncompliance with this Standard and submitted a Self-Report addressing this noncompliance, and ten days later, URE submitted its Self-Certification form marking "substantially compliant" with this Standard. Because URE filed the Self-Report after receiving the Self-Certification notice, WECC determined that the method of discovery is Self-Certification, not Self-Report. A few months later, URE submitted a second Self-Report further detailing the nature and cause of the violation.

WECC determined that URE had a violation of CIP-005-1 R3 because URE was not monitoring and logging access into the ESP containing URE's EMS and Substation and Physical Security System Networks. URE failed to implement and document an electronic or manual process for monitoring and logging authorized user accounts, and failed to detect and alert for attempts at or actual unauthorized accesses at URE's ESP.

WECC determined the duration of the violation to be from July 1, 2009, the date the Standard became enforceable for "Table 1" entities, through September 30, 2009, when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, URE's EMS, Substation and Physical Security networks are remotely accessible via Virtual Private Network and two-factor authentication. URE failed to implement and document monitoring, logging, detection, and alerting for actual or attempts at unauthorized access to such networks. In this instance, risk is associated with the lack of knowledge surrounding attempts at unauthorized access into the ESP. The entity would have been unaware of attempts by unauthorized users trying to access URE's ESP, thus allowing for unlimited access attempts by a potential attacker. The risk was not serious or substantial because URE did have secondary detection measures in place (*e.g.*, anti-virus, anti-malware, network-based detection technologies, and daily operations monitoring).

CIP-007-1 R5

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 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 "Lower" VRF.
WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process. URE self-reported violations of the Standard and after review, WECC determined that URE had a violation of CIP-007-1 R5 because URE: (1) failed to establish, implement, and document technical and procedural controls that minimize the risk of unauthorized system access; (2) failed to maintain historical audit trails of user account access for a minimum of ninety days; (3) failed to minimize and manage the scope and acceptable use of administrator, shared, factory default, and other generic accounts; and 4) failed to enforce complex passwords.

WECC determined the duration of the violation to be from July 1, 2009, the date the Standard became enforceable for "Table 1" entities, through August 28, 2009, when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to properly minimize unauthorized system access and enforce access authentication of, and accountability for, all user activity places an entity at an increased level of risk. An attacker may leverage known default vendor accounts to gain access to a critical system and compromise the security and reliability of the BPS. Non-complex passwords may also be exploited through brute force vectors utilizing dictionary attacks that seek out vulnerable password structures, thereby gaining access to critical systems through authorized accounts and compromised passwords. This risk was not serious or substantial because of URE's secondary detection measures in place (*e.g.*, anti-virus, anti-malware, network-based detection technologies, and daily operations monitoring) which mitigate the possible impact, along with URE's strong protections at the network layer.

CIP-007-1 R6 CIP-007-1 R6 provides:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible,

implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

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

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

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

CIP-007-1 R6 has a "Lower" VRF.
WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process. URE self-reported violations of the Standard and after review, WECC determined that URE had a violation of CIP-007-1 R6 because URE failed to implement Security Status Monitoring for all cyber assets within URE's ESPs. Specifically, URE failed to implement such tools and controls on four HMI PCs in URE's Substation ESP and 43 workstations and servers in URE's EMS ESP. URE failed to monitor less than 5 percent of its cyber assets within the ESPs.

WECC determined the duration of the violation to be from July 1, 2009, the date the Standard became enforceable for "Table 1" entities, through September 30, 2009, when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal risk to the reliability of the BPS and did not pose a serious or substantial risk. URE had secondary, compensating measures in place for the devices in scope of the violation. Specifically, the present violation is related to fewer than 5% of URE's applicable assets within the ESP. URE has network-level security in place across all its devices within the ESP. Further, for the assets associated with this violation, URE has host-based security status monitoring in place.

CIP-007-1 R1
CIP-007-1 R1 provides:

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For

purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

CIP-007-1 R1 has a "Medium" VRF.

WECC determined that URE had a violation of CIP-007-1 R1 because during the Spot Check, URE failed to show the Spot Check team that URE documented its test results in accordance with R1.3. URE's servers are within URE's ESP, and even though URE had significantly changed some servers within URE's ESP, it did not have documented test results as required by R1.3. URE did have test procedures in place for cyber assets and critical cyber assets within the electronic security perimeter in accordance with R1. Further, URE's test procedures were performed in a manner that minimized adverse effects on its production environment in accordance with R1.1. Finally, URE documented that its testing was performed in a manner that reflects the production environment in accordance with R1.2.

WECC determined the duration of the violation to be from July 1, 2008, the date the Standard became enforceable for "Table 1" entities, through December 15, 2010, when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, due to URE's failure to document test results, URE could not ensure that proposed changes to critical cyber assets were properly tested. Further, by not documenting test results, URE ran the risk that a new Cyber Asset or a significant change to existing Cyber Assets might adversely modify URE's existing cyber security controls. The risk to the BPS was not serious or substantial because URE has documented its Critical Cyber Assets, and does have testing procedures; the violation lies only in the failure to document the results of such tests.

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.
>
> R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

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

WECC determined that URE had a violation of CIP-003-1 R1 because during the Spot Check, the Spot Check team determined URE failed to document and implement a cyber security policy that addressed all requirements in Standards CIP-002 through CIP-009. The Spot Check team reviewed sixteen policies and procedure documents that URE created. The Spot Check team determined that as of the final documents, URE had documented and implemented a Cyber Security Policy that addressed the requirements in Standards CIP-002 through CIP-009, including provisions for emergency situations. URE corrected its noncompliance prior to the Spot Check.

WECC determined the duration of the violation to be from July 1, 2008, the date the Standard became enforceable for "Table 1" entities, through June 29, 2009, when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's Control Area Operations Department Policy provided a high-level framework for the security of URE's cyber systems, but failed to address all of the requirements of CIP-002 through CIP-009. Critical Cyber Assets must be protected in accordance with the CIP Standards to ensure continued operation of the BPS. While URE's Cyber Security Policy failed to address many of the requirements of CIP-002 through CIP-009, URE had secondary detection measures in place, and updated and corrected its Cyber Security Policy earlier in the audit period.

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 "Medium" VRF.

WECC determined that URE had a violation of CIP-004-1 R2 because during the Spot Check, the Spot Check team determined URE failed to provide cyber security training to 94.59% of its employees, contractors, and vendors with authorized unescorted physical or cyber access to URE's Critical Cyber Assets within 90 calendar days of such access being granted. The Spot Check team further determined URE failed to establish a Cyber Security Training Program that ensured employees, contractors, and vendors received training within 90 calendar days of gaining authorized unescorted physical access or cyber access to Critical Cyber Assets, and failed to perform an annual review of its initial Cyber Security Training Program. URE failed to create Cyber Security Training Program materials that addressed URE's policies and procedures addressing the proper use of Critical Cyber Assets. Finally, the Spot Check team determined URE failed to include material specific to URE's personnel roles and responsibilities in its training program.

WECC determined the duration of the violation to be from July 1, 2008, the date the Standard became enforceable for "Table 1" entities, through March 1, 2010, when URE completed its Mitigation Plan.

WECC determined that this violation posed a severe risk to the reliability of the BPS. Specifically, URE failed to provide adequate training to all personnel in a timely manner. In this case, URE's training practices could have led to URE's personnel not understanding or implementing URE's policies, access controls, and procedures improperly, producing an insecure environment for Critical Cyber Assets. Inadequate proper use of Critical Cyber Assets, proper handling of Critical Cyber Asset information (including handling of social engineering issues), and specific training on Cyber Security Incident Response and Critical Cyber Asset Recovery could have led to exploitation of personnel vulnerabilities with regard to Cyber Security. Such vulnerabilities can lead to the misuse of Cyber Assets. URE did have secondary detection measures in place (*e.g.*, anti-virus, anti-malware, network-based detection technologies, and daily operations monitoring).

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.

WECC determined that URE had a violation of CIP-004-1 R3 because during the Spot Check, the Spot Check team identified 29% of individuals with unescorted physical and cyber access to URE's Critical Cyber Assets, who had not received a Personnel Risk Assessment within thirty days of being granted such access. The Spot Check team also identified one case where URE failed to conduct a seven-year criminal check. The Spot Check team noted that in that one case, URE had previously conducted the individual's background check in September 2001; the employee was due for a seven-year criminal check in September 2008, but retired in October 2008 without having undergone the seven-year criminal check. This violation is URE's second assessed violation of this Standard.

WECC determined the duration of the violation to be from July 1, 2008, the date the Standard became enforceable for "Table 1" entities, through March 9, 2010, when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS but did not pose a serious or substantial risk. Specifically, URE's failure to conduct Personnel Risk Assessments could lead to intentional or unintentional misuse of URE's Critical Cyber Assets or otherwise make such Assets vulnerable to attack. Although URE failed to conduct one seven-year criminal check, the employee involved retired within a month of the seven-year period ending. The employees involved were long-term employees with longstanding employment histories.

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 "Lower" VRF.

WECC determined that URE had a violation of CIP-004-1 R4 because the Spot Check team determined, based on a review of URE's evidence and responses to subsequent data requests,

that URE did not provide a list or lists of specific electronic access rights for personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The Spot Check team asked what URE used when reviewing electronic access rights. URE stated it could generate such a list, but that when reviewing access rights, URE relied on its reviewer's knowledge of URE's employees. The Spot Check team determined that while URE could have generated a list to review, it had not generated such a list. Thus, it did not maintain such a list and or review it in accordance with the Standard.

WECC determined the duration of the violation to be from July 1, 2008, the date the Standard became enforceable for "Table 1" entities, through April 28, 2010, when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal risk to the reliability of the BPS and did not pose a serious or substantial risk. Specifically, URE's failure to maintain a list or lists of specific electronic access rights for personnel could lead to unauthorized system use based on legacy system access that is not removed due to personnel resignations, terminations, or changes in roles and responsibilities. Access rights must be strictly monitored and maintained to ensure only authorized personnel access Critical Cyber Assets. In this case, the risk was mitigated because: (1) URE maintained and reviewed physical access in accordance with the standard; and (2) URE had a small staff with longstanding employment histories; responsible employees had fundamental knowledge of those personnel who should have electronic access to Critical Cyber Assets.

CIP-009-1 R1

The purpose of Reliability Standard CIP-009-1 provides in pertinent part: "Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…"

CIP-009-1 R1 provides:

> R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:
>
> > R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).
> >
> > R1.2. Define the roles and responsibilities of responders.

CIP-009-1 R1 has a "Medium" VRF.

Based on the Spot Check, WECC determined that URE had a violation of CIP-009-1 R1 because URE's cyber security recovery plan that was in effect did not specify the required actions in

response to events or conditions of varying duration and severity that would activate the recovery plan.

WECC determined the duration of the violation to be from July 1, 2008, the date the Standard became enforceable for "Table 1" entities, through June 26, 2009, when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS but did not pose a serious or substantial risk. Specifically, the lack of specified direction may not allow for personnel to adequately respond to incidents that require the recovery of Critical Cyber Assets. This delayed response could render Critical Cyber Assets unavailable with an extended reduction in BPS reliability. URE did have a recovery plan including the roles and responsibilities of responders. Although URE's plan was deficient for the Standard, URE did have appropriate staff prepared to respond and restore its equipment as necessary. Further, URE had recovery procedures, but URE did not document the procedures in a manner consistent with the requirements of the Standard.

CIP-009-1 R2

CIP-009-1 R2 provides: "Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident."

CIP-009-1 R2 has a "Lower" VRF.

WECC determined that URE had a violation of CIP-009-1 R2 because URE failed to present evidence demonstrating that it had tested its recovery plan at least annually. Specifically, URE exercised its recovery plan for the first time on June 23, 2009. URE did not present evidence that it had tested its plan prior to the "Auditably Compliant" date. WECC Enforcement determined URE was required to have exercised the plan prior to its July 1, 2008, "Compliant" date per the NERC CIP Implementation Plan. URE corrected its noncompliance prior to the Spot Check.

WECC determined the duration of the violation to be from July 1, 2008, the date the Standard became enforceable for "Table 1" entities, through June 23, 2009, when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal risk to the reliability of the BPS and did not pose a serious or substantial risk. Specifically, although URE did not exercise its recovery plan as required, it did test its recovery plan on June 23, 2009. Such a testing schedule is not likely to have a significant impact on the reliability of the BPS because the recovery plan was ultimately tested and because URE tested the plan within a year of the Effective Date of the Standard.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred forty-three thousand five hundred dollars ($143,500) for the referenced violations. In reaching this

determination, WECC considered the following factors: (1) the seriousness of each violation, including the applicable VRF and Violation Severity Level, and the risk to the reliability of the BPS; (2) the violation's duration; (3) the Registered Entity's compliance history; (4) the Registered Entity's self-reports and voluntary corrective action;[13] (5) the degree and quality of cooperation by the Registered Entity in the audit or investigation process, and in any remedial action; (6) the quality of the Registered Entity's compliance program; (7) any attempt by the Registered Entity to conceal the violation or any related information; (8) whether the violation was intentional; (9) any other relevant information or extenuating circumstances; and (10) the Registered Entity's ability to pay a penalty.

After consideration of the above factors, and WECC's determination that three of the violations were minimal risks to the BPS, six of the violations were moderate risks to the BPS, and one violation represented a serious and substantial risk to the BPS, WECC determined that, in this instance, the penalty amount of one hundred forty-three thousand five hundred dollars ($143,500) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[14]

CIP-005-1 R3
URE's Revised Mitigation Plan to address its violation of CIP-005-1 R3 was submitted as complete to WECC on November 6, 2009 with a completion date of September 30, 2009. The Mitigation Plan was accepted by WECC on December 28, 2009 and approved by NERC on February 8, 2010. The Mitigation Plan for this violation is designated as MIT-09-2239 and was submitted as non-public information to FERC on February 9, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Complete, review, and implement an appropriate logging configuration to support R3.2.
2. Retain the logs and implement a manual log process so that at least once every ninety days, attempts at, or actual unauthorized access, is reviewed.
3. Install a software tool on the related authentication servers and configure it to send event logs to a centralized log server (already defined as a cyber asset).
4. Retain the centralized log server for at least ninety days and in real time, forward a copy of those events to a security and information manager appliance (already defined as a cyber asset).
5. Finally, use the security and information manager appliance to check the logs for attempts or actual unauthorized accesses and automatically issue alerts to the response personnel.

[13] Although three violations were self-reported, they did not receive self-reporting credit because they were treated as self-certifications.
[14] *See* 18 C.F.R § 39.7(d)(7).

URE certified on November 11, 2009 that the above Mitigation Plan requirements were completed on September 30, 2009. WECC reviewed URE's evidence of completion of its Mitigation Plan.

On February 9, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on September 30, 2009 and that URE was in compliance with CIP-005-1 R3.

CIP-007-1 R5

URE's Revised Mitigation Plan to address its violation of CIP-007-1 R5 was submitted as complete to WECC on November 6, 2009 with a completion date of August 28, 2009. The Mitigation Plan was accepted by WECC on December 28, 2009 and approved by NERC on February 8, 2010. The Mitigation Plan for this violation is designated as MIT-09-2238 and was submitted as non-public information to FERC on February 9, 2010 in accordance with FERC orders.

In accordance with its Mitigation Plan, URE:

1. URE completed implementation of the access log retention requirements and the account management controls, as necessary, in the Substations, EMS and Physical Security network Electronic Security Perimeters (ESPs) or documented any technical infeasibility where required.
2. With respect to R5.l.2, URE completed logging configuration changes on: (1) the authentication servers (one server within the EMS ESP and servers managing VPN and two factor authentication access to the Physical Security, EMS, and the Substations ESPs) and (2) network switches and routers within the EMS ESP to assure that the logs are maintained for a minimum of 90 days. Automated alerting of log events or 90-day review of logs was implemented based on which was necessary.
3. With respect to R5.2 and R5.3 within the Physical Security ESP, URE completed documentation regarding the technical infeasibility where it applied of following the requirements for the following cyber assets: (1) clients used to view cyber assets and (2) modules installed on the panels in the critical locations which interface the panels with the application server.
4. With respect to R5.2 and R5.3 within the EMS ESP, the EMS application password capabilities were documented with the technical infeasibility where it applied.
5. With respect to R5.2 and R5.3 within the Substations ESP, completed changes or documentation regarding technical infeasibility for password capabilities for: (1) HMIs, (2) Fault recorders, (3) modules, (4) network switches, (5) multiplexors and (6) one server.

URE certified on November 11, 2009 that the above Mitigation Plan requirements were completed on August 28, 2009. WECC reviewed URE's evidence of completion of its Mitigation Plan.

On February 9, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on August 28, 2009 and that URE was in compliance with CIP-007-1 R5.

CIP-007-1 R6

URE's Revised Mitigation Plan to address its violation of CIP-007-1 R6 was submitted as complete to WECC on November 6, 2009 with a completion date of September 30, 2009. The Mitigation Plan was accepted by WECC on December 28, 2009 and approved by NERC on February 8, 2010. The Mitigation Plan for this violation is designated as MIT-09-2240 and was submitted as non-public information to FERC on February 9, 2010 in accordance with FERC orders.

In accordance with its Mitigation Plan:

1. On the Substations network ESP, URE completed implementation of appropriate logging configurations using the local security policy on the four HMI PCs which are now manually reviewed for cyber security incidents per the requirements of the Standard.
2. On the EMS network ESP, URE completed implementation of appropriate logging configurations using the active directory group policy on the 43 workstations and servers which are now manually reviewed for cyber security incidents.
3. On the Physical Security ESP, URE completed installation of a software tool on the one Windows-based host and configured it to send events to a central log server (already a defined cyber asset). The log server is configured to retain the logs for at least ninety days and to forward a copy of these logs, in real time, to a security and information manager appliance. The security and information manager appliance checks these logs for cyber security incidents and automatically issues alerts to the response personnel.

URE certified on November 11, 2009 that the above Mitigation Plan requirements were completed on September 30, 2009. WECC reviewed URE's evidence of completion of its Mitigation Plan.

On February 9, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on September 30, 2009 and that URE was in compliance with CIP-007-1 R6.

CIP-007-1 R1

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to WECC on October 25, 2010 with a proposed completion date of December 15, 2010. The Mitigation Plan was accepted by WECC on November 4, 2010 and approved by NERC on November 24, 2010. The Mitigation Plan for this violation is designated as MIT-08-2981 and was submitted as non-public information to FERC on November 24, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review and revise the supporting documents to more clearly state the level of testing, the procedures for documenting test results and more clearly define the information required on each Change Plan Package to specifically identify each Cyber Asset tested, the test case applied during testing and the results of the test based on the test case criteria.

2. Ensure all personnel responsible for making or approving changes to Cyber Assets will be fully trained in the procedures and their responsibilities.

URE certified on January 19, 2011 that the above Mitigation Plan requirements were completed on January 19, 2011. WECC reviewed URE's evidence of completion of its Mitigation Plan

On June 27, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on January 19, 2011 and that URE was in compliance with CIP-007-1 R1.

CIP-003-1 R1
URE's Mitigation Plan to address its violation of CIP-003-1 R1 was submitted as complete to WECC on May 17, 2010 with a completion date of June 29, 2009. The Mitigation Plan was accepted by WECC on August 10, 2010 and approved by NERC on October 5, 2010. The Mitigation Plan for this violation is designated as MIT-08-2828 and was submitted as non-public information to FERC on October 6, 2010 in accordance with FERC orders.

In accordance with its Mitigation Plan, URE corrected its noncompliance prior to the Spot Check by documenting and implementing a series of policies, together encompassing the totality of the requirements of CIP-002 through CIP-009.

URE certified on May 19, 2010 that the above Mitigation Plan requirements were completed on June 29, 2009. WECC reviewed URE's evidence of completion of its Mitigation Plan.

On September 10, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on June 29, 2009 and that URE was in compliance with CIP-003-1 R1.

CIP-004-1 R2
URE's Mitigation Plan to address its violation of CIP-004-1 R2 was submitted as complete to WECC on May 17, 2010 with a completion date of March 1, 2010. The Mitigation Plan was accepted by WECC on October 6, 2010 and approved by NERC on November 5, 2010 The Mitigation Plan for this violation is designated as MIT-08-2956 and was submitted as non-public information to FERC on November 5, 2010 in accordance with FERC orders.

In accordance with URE's Mitigation Plan:

1. In June 2009, URE implemented new policies for Security Awareness and Training which ensure that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets have Cyber Security Training prior to being granted access.
2. Per URE's policy on security awareness and training, URE reviewed the Cyber Security training program and worked with its vendor to update its Cyber Security training program.

3. URE's Cyber Security training program materials contains provisions for the proper use of Critical Cyber Assets.

URE certified on May 19, 2010 that the above Mitigation Plan requirements were completed on March 1, 2010. WECC reviewed URE's evidence of completion of its Mitigation Plan.

On October 13, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on March 1, 2010 and that URE was in compliance with CIP-004-1 R2.

CIP-004-1 R3

URE's Mitigation Plan to address its violation of CIP-004-1 R3 was submitted as complete to WECC on May 17, 2010 with a completion date of June 29, 2009. The Mitigation Plan was accepted by WECC on September 22, 2010 and approved by NERC on October 8, 2010. The Mitigation Plan for this violation is designated as MIT-08-2877 and was submitted as non-public information to FERC on October 8, 2010 in accordance with FERC orders.

In accordance with URE's Mitigation Plan:

1. URE has fully implemented policy on personnel risk management, the Human Resources personnel risk assessment program, and the Corporate Security CIP personnel risk assessment program.
2. URE had PRAs performed for the employees who had not received them within 30 days of access.
3. The HR department and person assigned to oversee and manage the PRA process will monitor the CIP eligible personnel worksheet on an annual basis and review the background check expiration dates for all CIP-eligible employees to determine when an employee requires a new background check for the purpose of re-certification under the PRA process and applicable CIP Standard.
4. The HR department will calendar the annual review and, where an employee's PRA is scheduled to expire, the HR Department will send an email alert prior to the expiration of such background check to the employee and the managing supervisor to remind them of the need to resubmit the necessary forms to authorize HR to update the PRA.
5. Corporate Security is primarily responsible for conducting background checks on all contractors and service vendors who require cyber or unescorted physical access to Critical Cyber Assets through its third-party investigative service.
6. Corporate Security maintains an electronic list for contractor and service vendor PRAs, sorted by date. Corporate Security reviews PRA dates annually to ensure PRAs for all contractor and service vendors will be completed within the seven-year period.

URE certified on September 17, 2010 that the above Mitigation Plan requirements were completed on March 9, 2010. WECC reviewed URE's evidence of completion of its Mitigation Plan.

On October 6, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on March 9, 2010 and that URE was in compliance with CIP-004-1 R3.

CIP-004-1 R4

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted as complete to WECC on May 17, 2010 with a completion date of April 28, 2010. The Mitigation Plan was accepted by WECC on September 22, 2010 and approved by NERC on October 8, 2010. The Mitigation Plan for this violation is designated as MIT-08-2878 and was submitted as non-public information to FERC on October 8, 2010 in accordance with FERC orders.

In accordance with URE's Mitigation Plan:

1. In June 29, 2009, URE implemented policies and supporting documents for reviewing and maintaining access lists for personnel with electronic access to Critical Cyber Assets.
2. URE created a separate list that shows electronic Access and unescorted physical access to Critical Cyber Assets.
3. The quarterly reviews of electronic access are documented using URE's policy on access and privileges.

URE certified on May 19, 2010 that the above Mitigation Plan requirements were completed on April 28, 2010. WECC reviewed URE's evidence of completion of its Mitigation Plan.

On October 1, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on April 28, 2010 and that URE was in compliance with CIP-004-1 R4.

CIP-009-1 R1

URE's Mitigation Plan to address its violation of CIP-009-1 R1 was submitted as complete to WECC on May 17, 2010 with a completion date of June 26, 2009. The Mitigation Plan was accepted by WECC on August 19, 2010 and approved by NERC on October 5, 2010. The Mitigation Plan for this violation is designated as MIT-08-2829 and was submitted as non-public information to FERC on October 6, 2010 in accordance with FERC orders.

URE corrected its noncompliance prior to the Spot Check. Specifically, URE implemented new policies and supporting documentation that addressed CIP-009-2 R1. URE's recovery plan specified the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan and defined the roles and responsibilities of responders.

URE certified on May 19, 2010 that the above Mitigation Plan requirements were completed on June 26, 2009. WECC reviewed URE's evidence of completion of its Mitigation Plan.

On September 10, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on June 26, 2009 and that URE was in compliance with CIP-009-1 R1.

CIP-009-1 R2

URE's Mitigation Plan to address its violation of CIP-009-1 R2 was submitted as complete to WECC on May 17, 2010 with a completion date of June 23, 2009. The Mitigation Plan was accepted by WECC on August 19, 2010 and approved by NERC on October 5, 2010. The Mitigation Plan for this violation is designated as MIT-08-2830 and was submitted as non-public information to FERC on October 6, 2010 in accordance with FERC orders.

In accordance with URE's Mitigation Plan:

1. URE exercised its recovery plan in June 2009 which was between the period of July 1, 2008 and June 30, 2009.
2. In addition to the recovery exercise, URE performed six recovery exercises during the period of July 1, 2008 through June 30, 2009.

URE certified on May 19, 2010 that the above Mitigation Plan requirements were completed on June 23, 2009. WECC reviewed URE's evidence of completion of its Mitigation Plan.

On September 10, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on June 23, 2009 and that URE was in compliance with CIP-009-1 R2.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[15]

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,[16] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on May 9, 2011. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred forty-three thousand five hundred dollar ($143,500) 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.

[15] *See* 18 C.F.R. § 39.7(d)(4).

[16] *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).

In reaching this determination, the NERC BOTCC considered the following factors:[17]

1. WECC reported that URE was cooperative throughout the compliance enforcement process;
2. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
3. WECC determined that the CIP-004-1 R2 violation posed a severe risk to the reliability of the BPS and six of other violations posed a moderate risk to the BPS;
4. WECC determined that the remaining violations did not pose a serious or substantial risk to the reliability of the BPS; and
5. 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 forty-three thousand five hundred dollars ($143,500) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

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

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

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

[17] URE did not receive credit for having a compliance program because URE was just developing an ICP at the time of the URE last Compliance Audit in 2008 and it was not re-reviewed by WECC.

Attachments to be Included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between WECC and URE executed February 14, 2011, included as Attachment a;

b) Record documents for the violation of CIP-005-1 R3, included as Attachment b:

i. URE's source documents;

ii. URE's Revised Mitigation Plan designated as MIT-09-2239;

iii. URE's Certification of Mitigation Plan Completion;

iv. WECC's Verification of Mitigation Plan Completion;

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

i. URE's source documents;

ii. URE's Revised Mitigation Plan designated as MIT-09-2238;

iii. URE's Certification of Mitigation Plan Completion;

iv. WECC's Verification of Mitigation Plan Completion;

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

i. URE's source documents;

ii. URE's Revised Mitigation Plan designated as MIT-09-2240;

iii. URE's Certification of Mitigation Plan Completion;

iv. WECC's Verification of Mitigation Plan Completion;

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

i. URE's source documents;

ii. URE's Revised Mitigation Plan designated as MIT-08-2981;

iii. URE's Certification of Mitigation Plan Completion;

iv. WECC's Verification of Mitigation Plan Completion dated June 27, 2011;

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

i. URE's source documents;

ii. URE's Revised Mitigation Plan designated as MIT-08-2828;

iii. URE's Certification of Mitigation Plan Completion;

iv. WECC's Verification of Mitigation Plan Completion;

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

i. URE's source documents;

ii. URE's Revised Mitigation Plan designated as MIT-08-2956;

iii. URE's Certification of Mitigation Plan Completion;

iv. WECC's Verification of Mitigation Plan Completion;

h) Record documents for the violation of CIP-004-1 R3, included as Attachment h:

i. URE's source documents;

ii. URE's Revised Mitigation Plan designated as MIT-08-2877;

iii. URE's Certification of Mitigation Plan Completion;

iv. WECC's Verification of Mitigation Plan Completion;

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

i. URE's source documents;

ii. URE's Revised Mitigation Plan designated as MIT-08-2878;

iii. URE's Certification of Mitigation Plan Completion;

iv. WECC's Verification of Mitigation Plan Completion;

j) Record documents for the violation of CIP-009-1 R1, included as Attachment j:

i. URE's source documents;

ii. URE's Revised Mitigation Plan designated as MIT-08-2829;

iii. URE's Certification of Mitigation Plan Completion;

iv. WECC's Verification of Mitigation Plan Completion;

k) Record documents for the violation of CIP-009-1 R2, included as Attachment k:

i. URE's source documents;

ii. URE's Revised Mitigation Plan designated as MIT-08-2830;

iii. URE's Certification of Mitigation Plan Completion;

iv. WECC's Verification of Mitigation Plan Completion.

A Form of Notice Suitable for Publication[18]

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

[18] *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 David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters 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
Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 713-9598 (801) 582-3918 – facsimile Mark@wecc.biz	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	*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.
Sandy Mooy* Senior Legal 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	

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
David N. Cook
Sr. Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel for Corporate and Regulatory Matters
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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments