

January 31, 2013

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

**Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity
FERC Docket No. NP13-_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty¹ 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

Western Electricity Coordinating Council (WECC) performed an off-site audit of URE and determined that URE was in violation³ of PRC-005-1 R1 because URE's Generator Protection System Maintenance and Testing Program (Program) did not adequately define the maintenance and testing intervals and the basis for these intervals for voltage and current sensing devices and for DC control circuitry. Also, the Program did not contain a sufficient summary of maintenance and testing procedures in the documentation related to URE's voltage and current sensing protection system devices and DC control circuitry devices, in violation of this standard.

¹Rules 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.

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 2

Based on the same audit, WECC determined that URE failed to implement its Program for Potential Transformers (PTs), Current Transformers (CTs), and DC circuitry, including maintenance and testing within defined intervals, in violation of PRC-005-1 R2.

URE self-reported a violation of CIP-005-1 R1. WECC performed an off-site audit and determined that URE failed to document its testing procedures and a security patch management program for Cyber Assets used in the access control and monitoring of the Electronic Security Perimeters (ESPs) at one of its facilities, in violation of this Standard.

URE also self-reported a violation of CIP-006-1 R1. WECC performed an off-site audit and determined that URE failed to provide protection to the physical access control systems located in the computer room, in violation of CIP-006-1 R1.8.

URE also self-reported a violation of CIP-007-1 R1. WECC performed an off-site audit and determined that URE failed to perform security testing for any significant changes made on Cyber Assets within the ESP, and failed to establish and apply a security baseline in order to verify that no adverse effects had occurred after a significant change has been implemented, in violation of CIP-007-1 R1.

URE also self-reported a violation of CIP-007-1 R3. WECC performed an off-site audit and determined that URE failed to document security patches within 30 calendar days of the availability of the patches or upgrades, in violation of CIP-007-1 R3.1.

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 PRC-005-1 R1, PRC-005-1 R2, CIP-005-1 R1, CIP-006-1 R1.8, CIP-007-1 R1, and CIP-007-1 R3.1. According to the Settlement Agreement, URE agrees that the violations addressed hereby may be treated as confirmed violations and has agreed to the assessed penalty of one hundred fifteen thousand dollars (\$115,000), 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 WECC201102413, WECC201102414, WECC201102693, WECC201102689, WECC201102687, and WECC201102691 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 October 24, 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

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 3

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	1030	WECC201102413	PRC-005-1	1	High ⁴	115,000
			WECC201102414	PRC-005-1	2	High ⁵	
			WECC201102693	CIP-005-1	1	Medium ⁶	

⁴ When NERC filed VRFs for PRC-005-1, NERC originally assigned a Medium VRF to PRC-005-1 R1. In the Commission's May 18, 2007 Order on Violation Risk Factors, the Commission approved the VRF as filed but directed modifications. On June 1, 2007, NERC filed a modified High VRF for PRC-005 R1 for approval. On August 9, 2007, the Commission issued an Order approving the modified VRF. Therefore, the Medium VRF was in effect from June 18, 2007 until August 9, 2007 and the High VRF has been in effect since August 9, 2007.

⁵ PRC-005-1 R2 has a Lower Violation Risk Factor (VRF); R2.1 and R2.2 each have a High VRF. During a final review of the standards subsequent to the March 23, 2007 filing of the Version 1 VRFs, NERC identified that some standards requirements were missing VRFs; one of these include PRC-005-1 R2.1. On May 4, 2007, NERC assigned PRC-005 R2.1 a High VRF. In the Commission's June 26, 2007 Order on Violation Risk Factors, the Commission approved the PRC-005-1 R2.1 High VRF as filed. Therefore, the High VRF was in effect from June 26, 2007. In the context of this case, WECC determined that the violation related to both R2.1 and R2.2, and therefore a High VRF is appropriate.

⁶ CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a Medium VRF; R1.6 has a Lower VRF. When NERC filed VRFs it originally assigned CIP-005-1 R1.1, R1.2, R1.3, R1.4 and R1.5 Lower VRFs. 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 VRFs for CIP-005-1 R1.1, R1.2, R1.3, and R1.4 and on August 20, 2009, the Commission approved the modified Medium VRF for CIP-005-1 R1.5. Therefore, the Lower VRFs for CIP-005-1 R1.1, R1.2, R1.3, and R1.4 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective and the Lower VRF for CIP-005-1 R1.5 was in effect from June 18, 2007 until August 20, 2009 when the Medium VRF became effective.

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 4

			WECC201102689	CIP-006-1	1.8	Lower ⁷	
			WECC201102687	CIP-007-1	1	Medium ⁸	
			WECC201102691	CIP-007-1	3.1	Lower	

PRC-005-1 R1 (WECC201102413)

The purpose of Reliability Standard PRC-005-1 provides: “To ensure all transmission and generation Protection Systems^[9] affecting the reliability of the Bulk Electric System (BES) are maintained and tested.” (Footnote added.)

PRC-005-1 R1 provides:

R1. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:

R1.1. Maintenance and testing intervals and their basis.

R1.2. Summary of maintenance and testing procedures.

PRC-005-1 R1 has a High Violation Risk Factor (VRF) and a “Severe” Violation Severity Level (VSL).

WECC performed an off-site audit of URE, which included auditing compliance with PRC-005-1 R1. WECC’s determined that URE’s Program did not adequately define the maintenance and testing

⁷ CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a Medium VRF; R1.7, R1.8 and R1.9 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-006-1 R1.5 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-006-1 R1.5 was in effect from June 18, 2007 until February 2, 2009 when the Medium VRF became effective.

⁸ CIP-007-1 R1 has a Medium VRF and CIP-007-1 R1.2 and R1.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-007-1 R1.1 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-007-1 R1.1 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

⁹ *The NERC Glossary of Terms Used in Reliability Standards* defines Protection System as “Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry.”

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 5

intervals and the basis for these intervals for voltage and current sensing devices and for DC control circuitry.¹⁰ Also, the Program did not contain a sufficient summary of maintenance and testing procedures related to URE's voltage and current sensing protection system devices and DC control circuitry devices, in violation of PRC-005-1 R1.

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

WECC determined that this violation did not pose a serious or substantial risk and posed a minimal risk to the reliability of the bulk power system (BPS) because URE's Protection System equipment was being monitored continuously while the generators were operating. URE did perform maintenance and testing on some of its devices.

Status of Mitigation Plan¹¹

WECC Mitigation Plan to address its violation of PRC-005-1 R1.1 and R1.2 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT-00-5346 and was submitted as non-public information to FERC in accordance with FERC orders.

According to the Mitigation Plan, URE:

1. Revised its Plan to address the requirements of this Standard;
2. The Plan is now comprised of five elements- protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry, and the following requirements are applicable to each program element:
 - a. A documented defined interval for maintenance and testing;
 - b. A documented basis for setting the defined interval; and
 - c. A documented summary of the maintenance and testing procedures.

¹⁰WECC was unable to determine the total number or percentage of voltage and current sensing devices and DC control circuitry for which URE failed to define maintenance and testing intervals. URE stated that while its generators are "on" they are being continually monitored. However, URE could not provide WECC with any evidence of maintenance and testing records.

¹¹ See 18 C.F.R § 39.7(d)(7).

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 6

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted its Protection System Maintenance and Testing Program.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and notified URE in a letter.

PRC-005-1 R2 (WECC201102414)

PRC-005-1 R2 provides:

Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization^[12] on request (within 30 calendar days). The documentation of the program implementation shall include:

R2.1. Evidence Protection System devices were maintained and tested within the defined intervals.

R2.2. Date each Protection System device was last tested/maintained.

(Footnote added.)

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

Based on WECC's audit, which included auditing of URE's compliance of PRC-005-1 R2, WECC determined that URE failed to implement its Program for its PTs, CTs and DC control circuitry devices, including maintenance and testing within defined intervals.¹³ As a result, URE was unable to provide evidence that these devices were maintained and tested within defined intervals, in violation of this Standard.

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

¹² Consistent with applicable FERC precedent, the term "Regional Reliability Organization" in this context refers to WECC.

¹³ See Footnote 8.

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 7

WECC determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because, although a sporadic and inconsistent testing can undermine the reliability of the BPS, URE provided evidence that some PTs, CTs and DC control circuitry devices were tested since the implementation of its Program, indicating that URE was not ignoring the devices altogether. Also, URE's Program indicated that the devices were continuously monitored when the generator is in operation.

Status of Mitigation Plan

UREs Mitigation Plan to address its violation of PRC-005-1 R2 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT-00-5347 and was submitted as non-public information to FERC in accordance with FERC orders.

According to its Mitigation Plan, URE:

1. Developed a process for reviewing maintenance and testing activities to ensure that its Generation Protection System Maintenance and Testing Program is being adhered to by all URE's facilities; and
2. A team comprised of URE's generation personnel developed a procedure for documenting maintenance and testing activities as required by this Standard.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted its PRC-005-1 R2 testing overview spreadsheet, which identifies applicable protection system devices, test dates, and location of associated test results and the PRC-005-1 R2 test data.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and notified URE in a letter.

CIP-005-1 R1 (WECC201102693)

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."

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 8

CIP-005-1 R1 provides:

R1. Electronic Security Perimeter — The Responsible Entity¹⁴ 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

¹⁴ Within the text of Standard CIP-002 - 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.

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 9

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 VRF¹⁵ and a VSL was not applicable to this Standard.

URE self-reported a violation of CIP-005-1 R1 and CIP-007-1 R1 and R3. The possible violations in these Self-Reports were based on URE's misunderstanding of certain Reliability Requirements.¹⁶ WECC performed an off-site audit which included auditing of compliance with CIP-005-1 R1. Based on the entire record, WECC determined that URE failed to document its testing procedures and a security patch management program for Cyber Assets used in the access control and monitoring of the ESPs at a URE facility, in violation of this Standard.

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

WECC determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because, although failure to afford protective measures to Cyber Assets used in the access control and monitoring of the ESP may lead to malicious access to these assets, URE applied alternative security measures to these devices, as specified in CIP-003, CIP-004 R3, CIP-005 R2 and R3, CIP-006 R2 and R3, and CIP-007 R4 through R9, CIP-008 and CIP-009.

Status of Mitigation Plan

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as MIT-11-8305 and was submitted as non-public information to FERC in accordance with FERC orders.

According to its Mitigation Plan, URE:

1. Developed procedures for security testing and security patch management for Cyber Assets used in the access control and monitoring of the ESP;
2. Developed specific security tests and provided training to its personnel;

¹⁵ CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a Medium VRF; R1.6 has a Lower VRF.

¹⁶ The reports were based on a single act of non-compliance, namely URE's misunderstanding of certain Requirements. Because CIP-005-1 R1 references the Requirements of CIP-007-1 R1 and R3, URE Self-Report of CIP-007-1 R1 and R3 triggered the associated CIP-005-1 R1 Self-Report.

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 10

3. URE's security patch management now encompasses record retention, tracking, testing, and installation of the security patches;
4. URE purchased a patch management service to help track the availability of security patches; and
5. Training was provided to all appropriate personnel to ensure that procedures were implemented properly.

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

1. Procedures for security testing of Cyber Assets used in the access control and monitoring of the ESP;
2. Procedures for security patch management;
3. A spreadsheet showing the patch assessment and implementation;
4. Training documents on the new procedures; and
5. Attendance rosters.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and notified URE in a letter.

CIP-006-1 R1.8 (WECC201102689)

The purpose of Reliability Standard CIP-006-1 R1 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 R1 provides in pertinent part:

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 11

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

CIP-006-1 R1.8 has a Lower VRF¹⁷ and a VSL was not applicable to this Standard.

URE self-reported a violation of CIP-006-1 R1. WECC performed an off-site audit of URE, which included auditing compliance with CIP-006-1 R1. During the audit, WECC determined that URE could not provide evidence that it afforded all protective measures as specified in R1.8. Specifically, URE failed to provide the following protective measures related to a server, located in the computer room: Access Controls (CIP-005 R2), Monitoring Electronic Access (CIP-005 R3), and System Management (CIP-007 R1 through R9) to the server.

Based on the entire record, WECC determined that URE failed to provide protection to the Physical Access Control Systems at its Physical Access Control System, in violation of CIP-006-1 R1.8.

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

WECC determined that this violation did not pose a serious or substantial risk and posed a minimal risk to the reliability of the BPS because URE's existing strong physical security controls significantly reduced the risk on this device. Also, URE applies additional security measures as specified in CIP-003, CIP-004, CIP-006 R4 and R5, CIP-008 and CIP-009.

Status of Mitigation Plan

URE's Mitigation Plan to address its violation of CIP-006-1 R1.8 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as MIT-11-3832 and was submitted as non-public information to FERC in accordance with FERC orders.

According to the Mitigation Plan, URE:

1. Deployed electronic access controls for the cyber assets that authorized and/or log access to PSPs;
2. Installed multiple firewalls that create protected networks at the servers and at each card reader panel (the firewalls) 1) enabled only ports and services required for operations and

¹⁷ CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; R1.7 and R1.8 each have a "Lower" VRF.

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 12

- monitored by the cyber security administration team; 2) log electronic access to all cyber assets;
3. Documented the organizational process and technical and procedural mechanisms for electronic access control;
 4. Documented the electronic or manual processes for monitoring and logging access twenty-four hours a day, seven days a week;
 5. Documented and implemented the testing of cyber assets and significant changes to existing cyber assets that authorize and/or log access to the PSPs;
 6. Documented and implemented a procedure and process to ensure that only those ports and services required for normal operations are enabled for cyber assets that authorize and/or log access to the PSPs;
 7. Documented and implemented a security patch management program for cyber assets that authorized and/or log access to the PSPs;
 8. Documented and used the anti-virus software and malicious software prevention tools, where technically feasible, to detect, prevent, deter and mitigate the introduction, exposure, and a prorogation of malware on all cyber assets that authorize and/or log access to the PSPs;
 9. Documented and implemented procedural controls to authorize and enforce access authentication of and accountability for all user activity that will minimize the risk of unauthorized system access for cyber assets that authorize and/or log access to the PSPs;
 10. Configured all layer firewalls to generate sys logs for login activity and configuration changes;
 11. Captured the logs that were generated for user login, configuration changes and event acknowledgement;
 12. Documented and implemented security status monitoring by using the security information event management system for cyber assets that will monitor/alert system/security logs access to the PSPs;
 13. Documented and implemented formal methods, processes and procedures for disposal or deployment of cyber assets that authorize and/or log access to the PSPs;
 14. Documented and implemented a cyber vulnerability assessment program with annual testing for cyber assets using vulnerability penetration testing to verify that only ports and services required are enabled and control for accounts verified; and

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 13

15. Documented and implemented procedures to review and update all such documentation annually and whenever changes resulting from modifications to the systems or controls within thirty days for cyber assets that authorize and/or log access to the PSPs.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted its evidence matrix highlighting all protections missed in the evidence with corresponding evidence used to support compliance.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and notified URE in a letter.

CIP-007-1 R1 (WECC201102687)

The purpose of Reliability Standard CIP-007-1 R1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-007-1 R1 provides:

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

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

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

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

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 14

CIP-007-1 R1 has a Medium VRF¹⁸ and a VSL was not applicable to this Standard.

URE self-reported a violation of CIP-007-1 R1. WECC performed an off-site audit of URE which included auditing of URE's compliance with CIP-007-1 R1. WECC determined that URE failed to ensure that it adequately tested all Cyber Assets within the ESP. URE stated that it had misunderstood this Requirement and that it only performed functional tests¹⁹ when a significant change occurs to a Cyber Asset within the ESP and did not perform security tests,²⁰ as required by the Standard.

As a result, WECC determined that URE failed to perform security testing for any significant changes made on Cyber Assets within the ESP, and failed to establish and apply a security baseline in order to verify that no adverse effects had occurred after a significant change has been implemented, in violation of CIP-007-1 R1.

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

WECC determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because, although untested changes could introduce security vulnerabilities into URE's CCAs that are essential for the operation of the BPS, all patches applied to Distributed Control Systems (DCS) were tested by the DCS vendor and approved for installation prior to the actual installation.

Status of Mitigation Plan

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as MIT-11-3831 and was submitted as non-public information to FERC in accordance with FERC orders.

According to the Mitigation Plan, URE:

1. Revised its security test procedures to correctly verify the condition of the security baseline after a significant change has occurred;
2. Developed and documented a security baseline for each type of cyber asset within the ESP;

¹⁸ CIP-007-1 R1 and R1.1 each have a Medium VRF; R1.2 and R1.3 each have a "Lower" VRF.

¹⁹ Functional testing verifies that operations are not disrupted due to a change in Cyber Assets.

²⁰ Security testing requires the establishment of a security baseline and comparison of any significant change against the baseline to verify that no adverse affects have occurred as a result of any changes.

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 15

3. Documented the results of the testing in its electronic document management system, pursuant to URE's information protection program; and
4. Cyber security controls were tested to confirm and establish a baseline for the following: only those ports and services required for normal and emergency operations were enabled; anti-virus software protection, if any, is still effective; factory default accounts remain removed, disabled or renamed and for such accounts that must remain enabled, factory default passwords are not in effect; and logging and the security status monitoring system are properly enabled.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted test procedures, training documents, attendance documents, and testing documents.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and notified URE in a letter.

CIP-007-1 R3.1 (WECC201102691)

CIP-007-1 R3.1 provides:

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

CIP-007-1 has a Lower VRF and a VSL was not applicable to this Standard.

URE self-reported a violation of CIP-007-1 R3. WECC performed an off-site audit of URE, including auditing compliance with CIP-007-1 R3. WECC determined that URE failed to document the assessment of security patches within 30 days of availability for 83 Cyber Assets within URE's ESP. URE stated that its procedure for security patch management relied on a vendor to document the security

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 16

patches, but URE's CIP-007-1 R3 security patch management procedure stated that this task was the responsibility of the control systems group.

As a result, WECC determined that URE failed to document security patches within 30 calendar days of the availability of the patches or upgrades, in violation of CIP-007-1 R3.1.

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

WECC determined that this violation did not pose a serious or substantial risk and posed a minimal risk to the reliability of the BPS because URE did have a security patch management program for Cyber Assets in place even though it was relying on a vendor to assess and document the security patches.

Status of Mitigation Plan

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as MIT-11-3833 and was submitted as non-public information to FERC in accordance with FERC orders.

According to its Mitigation Plan, URE:

1. Developed and implemented security patch management procedures that require that security patches are assessed within thirty days of being available by a manufacturer; and
2. Purchased patch management service to facilitate and assist in the certification of patches and determination of applicability to URE's system.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted a CIP-007 R3 test procedure document.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and notified URE in a letter.

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 17

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed²¹

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,²² the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 12, 2011. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred fifteen thousand dollar (\$115,000) 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. Mitigating factors in determining the penalty amount:
 - a. URE's Internal Compliance Program (ICP) and continuous improvements of URE's compliance culture;
 - b. URE was cooperative throughout the process;
 - c. URE did not fail to complete any applicable compliance directives;
 - d. There was no evidence of any attempt by URE to conceal the violations;
 - e. For the violation of CIP-005-1 R1, CIP-006-1 R1, CIP-007-1 R1, and CIP-007-1 R3, WECC considered the fact that URE took voluntary corrective actions to remediate the violations and also gave URE partial self-reporting credit because URE submitted its Self-Reports within a week of WECC's Compliance audit.
 - f. URE had no reoccurring violations of these Standards, including PRC-005-1 R2, or relevant negative compliance history; and
 - g. There was no evidence that the violations were intentional.
2. Aggravating factors in determining the penalty amount:

²¹ See 18 C.F.R. § 39.7(d)(4).

²² *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).

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 18

- a. For PRC-005-1 R1, WECC determined that this violation should be treated as a repeat violation because one of URE's affiliates had previously violated this standard.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred fifteen thousand dollars (\$115,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

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

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

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

Attachments to be Included as Part of this Notice of Penalty

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

- a) Settlement Agreement by and between WECC and URE, included as Attachment a;
- b) Record documents for the violation of PRC-005-1 R1, included as Attachment b:
 - a. URE's Audit Report for PRC-005-1 R1;
 - b. TDMS's Mitigation Plan designated as MIT-00-5346;

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 19

- c. URE's Certification of Mitigation Plan Completion for PRC-005-1 R1; and
 - d. WECC's Verification of Mitigation Plan Completion for PRC-005-1 R1.
- c) Record documents for the violation of PRC-005-1 R2, included as Attachment c:
 - a. URE's Audit Report for PRC-005-1 R2;
 - b. TDMS's Mitigation Plan designated as MIT-00-5347;
 - c. URE's Certification of Mitigation Plan Completion; and
 - d. WECC's Verification of Mitigation Plan Completion.
- d) Record documents for the violation of CIP-005-1 R1, included as Attachment d:
 - a. URE's Self-Report;
 - b. URE's Mitigation Plan designated as MIT-11-3805;
 - c. URE's Certification of Mitigation Plan Completion; and
 - d. WECC's Verification of Mitigation Plan Completion.
- e) Record documents for the violation of CIP-006-1 R1.8, included as Attachment e:
 - a. URE's Self-Report;
 - b. URE's Mitigation Plan designated as MIT-11-3832;
 - c. URE's Certification of Mitigation Plan Completion; and
 - d. WECC's Verification of Mitigation Plan Completion.
- f) Record documents for the violation of CIP-007-1 R1, included as Attachment f:
 - a. URE's Self-Report;
 - b. URE's Mitigation Plan designated as MIT-11-3831;
 - c. URE's Certification of Mitigation Plan Completion; and
 - d. WECC's Verification of Mitigation Plan Completion.
- g) Record documents for the violation of CIP-007-1 R3.1, included as Attachment g:
 - a. URE's Self-Report;
 - b. URE's Mitigation Plan designated as MIT-11-3833;
 - c. URE's Certification of Mitigation Plan Completion; and
 - d. WECC's Verification of Mitigation Plan Completion.

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 20

A Form of Notice Suitable for Publication²³

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

²³ See 18 C.F.R § 39.7(d)(6).

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 21

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

<p>Gerald W. Cauley President and Chief Executive Officer 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326-1001</p> <p>Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile Charles.Berardesco@nerc.net</p> <p>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</p> <p>Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6885 (801) 883-6894 – facsimile CWhite@wecc.biz</p>	<p>Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters North American Electric Reliability Corporation 1325 G Street, N.W. Suite 600 Washington, DC 20005 (202) 400-3000 rebecca.michael@nerc.net</p> <p>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</p> <p>Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile RArredondo@wecc.biz</p> <p>*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.</p>
---	---

NERC Notice of Penalty
Unidentified Registered Entity
January 31, 2013
Page 22

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
Charles.Berardesco@nerc.net

Respectfully submitted,
/s/ Rebecca J. Michael
Rebecca J. Michael
Associate General Counsel for Corporate
and Regulatory Matters
North American Electric Reliability
Corporation
1325 G Street, N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
rebecca.michael@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments