PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 28, 2011

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

Re: NERC Abbreviated 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 Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Documents (Attachment b), 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 NOP is being filed with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations of CIP-005-1 R1 and R3, and CIP-007-1 R3.[3] According to the Settlement Agreement, URE agrees and stipulates to the facts of the violations and has agreed to the assessed penalty of thirty-five thousand dollars ($35,000), 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

[1] 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.
[2] *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).
[3] The Settlement Agreement uses CIP-007-1 and CIP-007-2 interchangeably; there are no substantive differences between versions of this standard. For purposes of this document and attachments hereto, CIP-007-1 version of the standard will be used.

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

violations identified as NERC Violation Tracking Identification Numbers WECC201002083, WECC201002085, and WECC201002077 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This NOP incorporates the findings and justifications set forth in the Settlement Agreement executed on March 2, 2011, by and between WECC and URE. The details of the findings and the basis for the penalty are set forth in the Disposition Documents. This NOP 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, NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
NOC-838	WECC201002083	CIP-005-1	1	Medium[4]	7/1/09-6/14/10[5]	35,000
	WECC201002085	CIP-005-1	3	Medium	7/1/09-4/28/10	
	WECC201002077	CIP-007-1	3	Lower	12/4/09-7/22/10	

The text of the Reliability Standards at issue and further information on the subject violations are set forth in the Disposition Documents.

CIP-005-1 R1 - OVERVIEW

URE submitted a Self-Report to WECC for this violation. WECC determined that URE did not identify and document all access points to Electronic Security Perimeters (ESPs).

CIP-005-1 R3 - OVERVIEW

URE submitted a Self-Report to WECC for this violation. WECC determined that URE did not monitor and document access to all ESPs according to its ESP monitoring procedure, and failed to review access logs at least every ninety calendar days.

CIP-007-1 R3 - OVERVIEW

URE submitted a Self-Report to WECC for this violation. WECC determined that although URE did have a Security Patch Management Process for all Cyber Assets in place, it had failed to assess and document all security patches within thirty days of availability. Further, URE did not document implementation of security patches, nor did URE document compensating measures in instances where the patch was not installed.

[4] CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each are assigned a "Medium" Violation Risk Factor (VRF) and CIP-005-1 R1.6 is assigned a Lower VRF.

[5] The Settlement Agreement contains a typographical error listing the Mitigation Plan completion date as September 13, 2010.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[6]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines, the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on June 10, 2011. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a thirty-five thousand dollar ($35,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. URE self-reported the violations;
2. WECC reported that URE was cooperative throughout the compliance enforcement process;
3. URE had a compliance program at the time of the violation which WECC considered a mitigating factor, as discussed in the Disposition Documents;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), as discussed in the Disposition Documents; and
6. 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 thirty-five thousand dollars ($35,000) 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 NOP with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

---

[6] *See* 18 C.F.R. § 39.7(d)(4).

[7] *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).

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 parts of this NOP are the following documents:

a) Settlement Agreement by and between WECC and URE executed March 2, 2011, included as Attachment a;

b) Disposition Document for Common Information, included as Attachment b;

   i. Disposition Document for CIP-005-1 R1 and R3, included as Attachment b-1; and

   ii. Disposition Document for CIP-007-1 R3, included as Attachment b-2;

c) URE Self-Report for CIP-005-1 R1, included as Attachment c;

d) URE Self-Report for CIP-005-1 R3, included as Attachment d;

e) URE Self-Report for CIP-007-1 R3, included as Attachment e;

f) URE Mitigation Plan MIT-09-2881 for CIP-005-1 R1, included as Attachment f;

g) URE Mitigation Plan MIT-09-2870 for CIP-005-1 R3, included as Attachment g;

h) URE Mitigation Plan MIT-09-2867 for CIP-007-1 R3, included as Attachment h;

i) URE Certification of Mitigation Plan Completion for CIP-005-1 R1, included as Attachment i;

j) URE Certification of Mitigation Plan Completion for CIP-005-1 R3, included as Attachment j;

k) URE Certification of Mitigation Plan Completion for CIP-007-1 R3, included as Attachment k;

l) WECC's Notice of Completed Mitigation Plan Acceptance for CIP-005-1 R1, included as Attachment l;

m) WECC's Notice of Completed Mitigation Plan Acceptance for CIP-005-1 R3, included as Attachment m; and

n) WECC's Notice of Completed Mitigation Plan Acceptance for CIP-007-1 R3, included as Attachment n.

A Form of Notice Suitable for Publication[8]

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

[8] *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 Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 213-2673 (801) 582-3918 – facsimile Mark@wecc.biz Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6855 (801) 883-6894 – facsimile CWhite@wecc.biz Sandy Mooy* Associate General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7658 (801) 883-6894 – facsimile SMooy@wecc.biz	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net 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 *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.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Abbreviated NOP 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
Associate General Counsel for Corporate and Regulatory Matters
Sonia C. Mendonça
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment b

Disposition Document for Common Information

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment b

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS

Dated June 10, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-838**

REGIONAL ENTITY
Western Electricity Coordinating Council (WECC)

IS THERE A SETTLEMENT AGREEMENT YES ☒ NO ☐

WITH RESPECT TO THE VIOLATION(S), REGISTERED ENTITY

NEITHER ADMITS NOR DENIES IT (SETTLEMENT ONLY) YES ☐
ADMITS TO IT YES ☒
Stipulates to the facts of the violation
DOES NOT CONTEST IT (INCLUDING WITHIN 30 DAYS) YES ☐

WITH RESPECT TO THE ASSESSED PENALTY OR SANCTION, REGISTERED ENTITY

ACCEPTS IT/ DOES NOT CONTEST IT YES ☒

I. PENALTY INFORMATION

TOTAL ASSESSED PENALTY OR SANCTION OF **$35,000** FOR **THREE** VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

PREVIOUSLY FILED VIOLATIONS OF ANY OF THE INSTANT RELIABILITY STANDARD(S) OR REQUIREMENT(S) THEREUNDER
YES ☐ NO ☐

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

[1] For purposes of this document and attachments hereto, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

PREVIOUSLY FILED VIOLATIONS OF OTHER RELIABILITY STANDARD(S) OR REQUIREMENTS THEREUNDER
YES ☐ NO ☐

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

(2) THE DEGREE AND QUALITY OF COOPERATION BY THE REGISTERED ENTITY (IF THE RESPONSE TO FULL COOPERATION IS "NO," THE ABBREVIATED NOP FORM MAY NOT BE USED.)

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

(3) THE PRESENCE AND QUALITY OF THE REGISTERED ENTITY'S COMPLIANCE PROGRAM

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ NO ☐ UNDETERMINED ☐
EXPLAIN
WECC reviewed URE' Internal Compliance Program (ICP) but applied minimal mitigating credit because the ICP should have prevented the repeat CIP violations. WECC reduced the mitigating credit for URE' ICP because of the repeat CIP violations.

EXPLAIN SENIOR MANAGEMENT'S ROLE AND INVOLVEMENT WITH RESPECT TO THE REGISTERED ENTITY'S COMPLIANCE PROGRAM, INCLUDING WHETHER SENIOR MANAGEMENT TAKES ACTIONS THAT SUPPORT THE COMPLIANCE PROGRAM, SUCH AS TRAINING, COMPLIANCE AS A FACTOR IN EMPLOYEE EVALUATIONS, OR OTHERWISE.

(4) ANY ATTEMPT BY THE REGISTERED ENTITY TO CONCEAL THE VIOLATION(S) OR INFORMATION NEEDED TO REVIEW, EVALUATE OR INVESTIGATE THE VIOLATION.

YES ☐ NO ☒
IF YES, EXPLAIN

(5) ANY EVIDENCE THE VIOLATION(S) WERE INTENTIONAL (IF THE RESPONSE IS "YES," THE ABBREVIATED NOP FORM MAY NOT BE USED.)

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

NOTICE OF ALLEGED VIOLATION AND PROPOSED PENALTY OR SANCTION ISSUED
DATE: **10/29/10** OR N/A ☐

SETTLEMENT REQUEST DATE
DATE: **12/10/10** OR N/A ☐

NOTICE OF CONFIRMED VIOLATION ISSUED
DATE: OR N/A ☒

SUPPLEMENTAL RECORD INFORMATION
DATE(S) OR N/A ☒

REGISTERED ENTITY RESPONSE CONTESTED
FINDINGS ☐ PENALTY ☐ BOTH ☐ DID NOT CONTEST ☒

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-005-1 R1 and R3

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment b-1

DISPOSITION OF VIOLATION

Dated June 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002083	**WECC2010-610376**
WECC201002085	**WECC2010-609953**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S) [1]
CIP-005-1	**1**		**Medium**[2]	**N/A**
CIP-005-1	**3**		**Medium**	**N/A**

PURPOSE OF THE RELIABILITY STANDARD AND TEXT OF RELIABILITY STANDARD AND REQUIREMENT(S)/SUB-REQUIREMENT(S)

The purpose statement of CIP-005-1 provides in pertinent part: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-005-1 R1 provides:

> **R1. Electronic Security Perimeter — The Responsible Entity[3] 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).**

[1] At the time of the violations, no Violation Severity Levels (VSLs) were in effect for CIP-005-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

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

[3] Within the text of Standard CIP-005, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

R1.2. 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 specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

(Footnote added.)

CIP-005-1 R3 provides:

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

VIOLATION DESCRIPTION

CIP-005-1 R1
URE submitted a Self-Report to WECC stating that even though it had taken steps to ensure that every Critical Cyber Asset (CCA) resided inside of an Electronic Security Perimeter (ESP), it had failed to identify and document all ESPs. URE reported that in implementing the Standard, URE construed ESP "access point(s)" to mean "physical access points to critical cyber assets such as USB ports and CD/DCD drives instead of logical access points."

A WECC Subject Matter Expert (SME) reviewed URE's Self-Report and determined that URE: (1) failed to identify all externally connected communication end points terminating at devices within the ESPs as access points per CIP-005-1 R1.1; (2) failed to identify CCAs using a non-routable protocol as an ESP access point per CIP-005-1 R1.2; (3) did not consider end points of a communication link within the ESP connecting discrete ESPs as ESP access points per CIP-005-1 R1.3; and (4) failed to document all ESPs, interconnected Critical and non-critical Cyber Assets within the ESPs, all electronic access points to the ESPs, and all Cyber Assets deployed for access control and monitoring of these access points per CIP-005-1 R1.6.

CIP-005-1 R3
URE submitted a Self-Report to WECC stating that although it implemented a process for manually monitoring and logging access to the ESP, it failed to monitor and document access to all ESPs. A WECC SME reviewed URE' ESP monitoring procedure which required personnel to manually review ESP access. URE reported that manual reviews of access to ESPs were not conducted or completed. URE also failed to review access logs every ninety calendar days as required by CIP-005 R3.2. The SME determined that URE failed to implement processes to monitor ESP access points. Further, because URE did not identify all ESP access points, all access was not monitored. URE's process for monitoring and logging access at access points to ESPs was not completed for any of the ESP access points. WECC Enforcement confirmed that URE implemented a new electronic monitoring system that addressed the non-compliance.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

CIP-005-1 R1
WECC determined that the violation posed a moderate risk to the reliability of the bulk power system (BPS) because failing to identify and document all ESP access points could expose CCAs to unscrupulous access attempts. WECC determined that the violation did not pose a serious or substantial risk to the reliability of the BPS because URE dial-up connections are physically disconnected from the EMS systems when not in use. During the period of non-compliance, URE did implement additional procedural controls providing some measure of security for dial-up controls. The URE network is an isolated physical network linking to the Balancing Authority via a secured, firewalled ICCP link.

CIP-005-1 R3
WECC determined that the violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because URE did implement processes for access monitoring. In addition to manual logging, URE implemented automatic electronic logging. Based on a comparison of the two programs (manual versus automatic electronic logging), URE identified shortfalls in its manual logging process and submitted the Self-Report. The violation was identified because the logging process was not consistent with URE' documented process including automatic electronic logging. Although these processes did not strictly conform to the requirement, they did provide some measure of protection and were effective as compensating measures.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT	☒
SELF-CERTIFICATION	☐
COMPLIANCE AUDIT	☐
COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK	☐
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

DURATION DATE(S)

CIP-005-1 R1: 7/1/09 through 6/14/10[4] (Mitigation Plan completion)

CIP-005-1 R3: 7/1/09 through 4/28/10 (Mitigation Plan completion)

[4] The Settlement Agreement contains a typographical error listing the Mitigation Plan completion date as September 13, 2010.

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY
CIP-005-1 R1 **Self-Report**
CIP-005-1 R3 **Self-Report**

IS THE VIOLATION STILL OCCURRING YES ☐ NO ☒
IF YES, EXPLAIN

REMEDIAL ACTION DIRECTIVE ISSUED YES ☐ NO ☒
PRE TO POST JUNE 18, 2007 VIOLATION YES ☐ NO ☒

III. MITIGATION INFORMATION

CIP-005-1 R1
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2881**
DATE SUBMITTED TO REGIONAL ENTITY	**6/15/10**
DATE ACCEPTED BY REGIONAL ENTITY	**9/16/10**
DATE APPROVED BY NERC	**10/8/10**
DATE PROVIDED TO FERC	**10/8/10**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**9/1/10**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**6/14/10**
DATE OF CERTIFICATION LETTER	**8/26/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**6/14/10**
DATE OF VERIFICATION LETTER	**9/24/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**6/14/10**[5]

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE revised its procedures to correctly document "access points" to CCAs contained within the URE ESP. URE revised procedures to identify the

[5] WECC's Verification Document incorrectly lists the completion date as September 13, 2010 when the Mitigation Plan completion date should be June 14, 2010.

access points correctly, as well as created a diagram that graphically represents the boundaries of the ESP and the access points to the ESP. URE will maintain and review the procedure at least annually to ensure it is accurate.

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED, LIST EVIDENCE REVIEWED FOR COMPLETED MILESTONES)

- **Electronic Security Perimeter access points and assets procedure that detailed the annual review and revision**
- **Critical Cyber Asset Access Point Diagram annual review and revision**
- **Non-Critical Cyber Asset Access Point Diagram annual review and revision**

CIP-005-1 R3

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2870**
DATE SUBMITTED TO REGIONAL ENTITY	**3/23/10**
DATE ACCEPTED BY REGIONAL ENTITY	**9/14/10**
DATE APPROVED BY NERC	**10/7/10**
DATE PROVIDED TO FERC	**10/7/10**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**4/30/10**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**4/28/10**
DATE OF CERTIFICATION LETTER	**4/29/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**4/28/10**
DATE OF VERIFICATION LETTER	**9/24/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**4/28/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE completed implementation of a automatic electronic logging platform, an electronic monitoring process configured to monitor access points and system events. URE updated its procedure for ESP access point monitoring, to include both automatic electronic logging monitoring and manual checks of automatic electronic logging monitoring. Finally, URE completed revisions to its procedure to include additional functionality

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED, LIST EVIDENCE REVIEWED FOR COMPLETED MILESTONES)

- **Security status monitoring procedure**

EXHIBITS:

SOURCE DOCUMENT
URE Self-Report for CIP-005-1 R1 URE Self-Report for CIP-005-1 R3

MITIGATION PLAN
URE Mitigation Plan MIT-09-2881 for CIP-005-1 R1
URE Mitigation Plan MIT-09-2870 for CIP-005-1 R3

CERTIFICATION BY REGISTERED ENTITY
URE Certification of Mitigation Plan Completion for CIP-005-1 R1
URE Certification of Mitigation Plan Completion for CIP-005-1 R3

VERIFICATION BY REGIONAL ENTITY
WECC's Notice of Completed Mitigation Plan Acceptance for CIP-005-1 R1
WECC's Notice of Completed Mitigation Plan Acceptance for CIP-005-1 R3

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007-1 R3

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment b-2

DISPOSITION OF VIOLATION

Dated June 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002077	**WECC2010-609954**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S) [1]
CIP-007-1 [2]	**3**		**Lower**	**N/A**

PURPOSE OF THE RELIABILITY STANDARD AND TEXT OF RELIABILITY STANDARD AND REQUIREMENT(S)/SUB-REQUIREMENT(S)

The purpose statement of CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities[3] 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." Footnote added.

CIP-007-1 R3 provides:

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

[1] At the time of the violations, no Violation Severity Levels (VSLs) were in effect for CIP-007-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[2] The Settlement Agreement uses CIP-007-1 and CIP-007-2 interchangeably; there are no substantive differences between versions of this standard. For purposes of this document and attachments hereto, CIP-007-1 version of the standard will be used.

[3] Within the text of Standard CIP-007, "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.

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

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

VIOLATION DESCRIPTION

URE submitted a Self-Report to WECC stating that although URE did have a Security Patch Management process for all Cyber Assets in place, it had failed to assess and document all security patches within thirty days of availability. URE had failed to strictly adhere to the program created as a part of the prior Mitigation Plan. Further, URE did not document implementation of security patches, nor did URE document compensating measures in instances where the patch was not installed. URE explained that the failure to adhere to the Security Patch Management process was due to turnover in personnel which had impacted who would be responsible for managing the process.

A WECC Subject Matter Expert (SME) reviewed the Self-Report and contacted URE. The SME determined that URE did not assess security patches for twenty-one Windows devices including workstations and servers, and two firewalls located in the URE Control Center.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the violation posed a minimal and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because URE has an isolated physical network which links only to the Balancing Authority via a secured, firewalled ICCP link. In addition, there were compensating measures in place to detect misuse and prevent malicious attack. The violation involved a discrete set of cyber assets and was not endemic on the whole system. URE only failed to assess patches for a five month period (December 3, 2009 through May 25, 2010). Finally, the vendor of the patch management system assesses current patches and would have notified URE of patches for systems and vulnerabilities and whether they would have impacted the system. The violation in this case was due to URE not documenting and running its own impact assessment in accordance with its Security Patch Management process.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT	☒
SELF-CERTIFICATION	☐
COMPLIANCE AUDIT	☐
COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK	☐
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

DURATION DATE(S) **12/4/09 (when URE failed to implement and document the security management patch process) through 7/22/10 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **Self-Report**

IS THE VIOLATION STILL OCCURRING	YES	☐	NO	☒
IF YES, EXPLAIN				
REMEDIAL ACTION DIRECTIVE ISSUED	YES	☐	NO	☒
PRE TO POST JUNE 18, 2007 VIOLATION	YES	☐	NO	☒

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2867**
DATE SUBMITTED TO REGIONAL ENTITY	**5/25/10**
DATE ACCEPTED BY REGIONAL ENTITY	**9/9/10**
DATE APPROVED BY NERC	**10/7/10**
DATE PROVIDED TO FERC	**10/7/10**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**7/25/10**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**7/22/10**
DATE OF CERTIFICATION LETTER	**7/22/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**7/22/10**

DATE OF VERIFICATION LETTER **9/20/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **7/22/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE personnel responsible for Patch Management have been trained and are knowledgeable of the requirements of CIP-007 R3. In the process of implementing the procedure for Patch Management, URE identified procedural revisions that addressed the prevention of future noncompliance more efficiently. URE revised its procedure for Patch Management to reflect the processes accurately, including the addition of the Patch Management Program provided by the EMS Vendor and any manual processes for assets not covered by the Patch Management Program. In addition, URE compiled a list of security patches previously made available for applicable assets from the in-service date to present. URE analyzed, tested, and installed the patches on assets. Where patches were not installed, compensating measures have been documented.

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED, LIST EVIDENCE REVIEWED FOR COMPLETED MILESTONES)

- **Security Patch Management process**
- **A spreadsheet filing containing URE's security updates for mitigation**

EXHIBITS:

SOURCE DOCUMENT
URE Self-Report for CIP-007-1 R3

MITIGATION PLAN
URE Mitigation Plan MIT-09-2867 for CIP-007-1 R3

CERTIFICATION BY REGISTERED ENTITY
URE Certification of Mitigation Plan Completion for CIP-007-1 R3

VERIFICATION BY REGIONAL ENTITY
WECC's Notice of Completed Mitigation Plan Acceptance for CIP-007-1 R3