NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

**PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION**

March 30, 2011

Ms. Kimberly 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 i), 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 enforceable violations of CIP-001-1 Requirement (R) 1 and R2; CIP-004-1 R2 and R3; CIP-006-1 R1; CIP-007-1 R1 and R5; and CIP-008-1 R1. According to the Settlement Agreement, URE neither admits nor denies the violations, but 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

[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 (2010). *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).

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

compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC200901259, WECC200901260, WECC200901625, WECC200901423, WECC200901644, WECC200801706, WECC200901491 and WECC200801185 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 July 6, 2010, 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-596 | WECC200901259 | CIP-001-1 | 1 | Medium | 7/23/08-1/16/09 | 35,000 |
| | WECC200901260 | CIP-001-1 | 2 | Medium | 7/23/08-1/16/09 | |
| | WECC200901625 | CIP-004-1 | 2/2.3 | Lower[3] | 7/19/09-7/21/09 | |
| | WECC200901423 | CIP-004-1 | 3 | Medium[4] | 7/1/08-4/23/09 | |
| | WECC200901644 | CIP-006-1 | 1/1.8 | Lower[5] | 7/1/09-11/18/09 | |
| | WECC200801706 | CIP-007-1 | 1 | Lower[6] | 7/1/08-1/30/09 | |
| | WECC200901491 | CIP-007-1 | 5 | Medium[7] | 7/1/09-11/25/09 | |
| | WECC200801185 | CIP-008-1 | 1/1.3 | Lower | 7/28/08-11/20/08 | |

[3] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" Violation Risk Factor (VRF); R2.1, R2.2 and R2.2.4 each have a "Medium" VRF.

[4] 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.

[5] 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. In the context of this case, WECC determined the violation related to R1.8 and therefore a "Lower" VRF is appropriate.

[6] CIP-007-1 R1 and R1.1 each have a "Medium" VRF; R1.2 and R1.3 each have a "Lower" VRF. In the context of this case, WECC determined the violation related to R1.2 and therefore a "Lower" VRF is appropriate.

[7] CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, R5.2.2, R5.3, R5.3.1 and R5.3.2 each have a "Lower" VRF; R5.1, R5.1.3, R5.2.1 and R5.2.3 each have a "Medium" VRF. In the context of this case, WECC determined the violation related to R5.1.2 and R5.2.1 and therefore a "Medium" VRF is appropriate.

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

CIP-001-1 R1 and R2 - OVERVIEW
On January 9, 2009, URE self-reported violations of CIP-001-1 R1 and R2, after purchasing a facility and assuming responsibility for this facility. WECC determined that URE did not have an adequate written procedure for the recognition of sabotage events at the facility as required by R1. Also, the facility did not have written procedures for the communication of information concerning sabotage events to appropriate parties within the Interconnection as required by R2.

CIP-004-1 R2 - OVERVIEW
On July 31, 2009, URE self-reported a violation of CIP-004-1 R2. WECC determined that URE, as a Responsible Entity,[8] did not maintain and document an annual cyber security training program for an individual who had physical access to a Physical Security Perimeter (PSP) surrounding a Critical Cyber Asset location, as required by R2.3.

CIP-004-1 R3 - OVERVIEW
On April 13, 2009, URE self-reported a violation of CIP-004-1 R3. WECC determined that URE, as a Responsible Entity, did not follow its documented personnel risk assessment program for a number of individuals with authorized access to Critical Cyber Assets.

CIP-006-1 R1 - OVERVIEW
On June 30, 2009, URE self-reported a violation of CIP-006-1 R1. WECC determined that URE, as a Responsible Entity, did not have a Physical Security Plan in place with all of the protective measures (required by CIP-005-1 and CIP-007-1) for its system for physical access control and monitoring associated with the PSP, as required by R1.8.

CIP-007-1 R1 - OVERVIEW
On December 29, 2008, URE self-reported a violation of CIP-007-1 R1. WECC determined that URE, as a Responsible Entity, did not have adequate cyber security test procedures and failed to perform and document testing in six known circumstances.

CIP-007-1 R5 - OVERVIEW
On June 9, 2009, URE self-reported a violation of CIP-007-1 R5. WECC determined that URE, as a Responsible Entity, did not 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, as required by R5.1.2. Also, URE did not include in its policy two Critical Cyber Assets that must remain enabled, as required by R5.2.1.

[8] 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.

CIP-008-1 R1 - OVERVIEW

On August 12, 2008, URE self-reported a violation of CIP-008-1 R1. WECC determined that URE, as a Responsible Entity, did not initiate its Cyber Security Incident response plan during a reportable event by ensuring that the Cyber Security Incident was reported to the Electricity Sector Information Sharing and Analysis Center (ES ISAC) either directly or through an intermediary, as required by R1.3.

**Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed**[9]

**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,[10] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2010. 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 violations, which WECC considered a mitigating factor, as discussed in the Disposition Document;
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. The NERC BOTCC approved the assessed penalty of thirty five thousand dollars ($35,000) as appropriate

[9] *See* 18 C.F.R. § 39.7(d)(4).

[10] *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).

for the violations and circumstances at issue, and 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.

**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 NOP are the following documents:

a) Settlement Agreement by and between WECC and URE executed July 6, 2010, included as Attachment a;

b) Record Documents for CIP-001-1 R1 and R2:

   i. URE's Self-Report for CIP-001-1 R1 dated January 9, 2009, included as Attachment b-1;

   ii. URE's Self-Report for CIP-001-1 R2 dated January 9, 2009, included as Attachment b-2;

   iii. URE's Mitigation Plan MIT-09-1429 submitted January 9, 2009 and signed January 12, 2009, included as Attachment b-3;

   iv. URE's Certification of Mitigation Plan Completion dated January 21, 2009, included as Attachment b-4; and

   v. WECC's Verification of Mitigation Plan Completion dated February 19, 2009, included as Attachment b-5.

c) Record Documents for CIP-004-1 R2:

   i. URE's Self-Report dated July 31, 2009, included as Attachment c-1;

ii. URE's Mitigation Plan MIT-09-1993 submitted August 10, 2009, included as Attachment c-2;

iii. URE's Certification of Mitigation Plan Completion dated September 4, 2009, included as Attachment c-3; and

iv. WECC's Verification of Mitigation Plan Completion dated November 9, 2009, included as Attachment c-4.

d) Record Documents for CIP-004-1 R3:

i. URE's Self-Report dated April 13, 2009 and revised April 23, 2009, included as Attachment d-1;

ii. URE's Mitigation Plan MIT-09-2029 submitted April 23, 2009, included as Attachment d-2;

iii. URE's Certification of Mitigation Plan Completion dated April 28, 2009, included as Attachment d-3; and

iv. WECC's Verification of Mitigation Plan Completion dated November 9, 2009, included as Attachment d-4.

e) Record Documents for CIP-006-1 R1:

i. URE's Self-Report dated June 30, 2009 and revised September 8, 2009, included as Attachment e-1;

ii. URE's Mitigation Plan MIT-09-2015 originally submitted June 30, 2009 and revised September 8, 2009, included as Attachment e-2;

iii. URE's Certification of Mitigation Plan Completion dated December 7, 2009, included as Attachment e-3; and

iv. WECC's Verification of Mitigation Plan Completion dated June 8, 2010, included as Attachment e-4.

f) Record Documents for CIP-007-1 R1:

i. URE's Self-Report dated December 29, 2008, included as Attachment f-1;

ii. URE's Mitigation Plan MIT-08-2125 submitted January 8, 2009, included as Attachment f-2;

iii. URE's Certification of Mitigation Plan Completion dated February 2, 2009, included as Attachment f-3; and

iv. WECC's Verification of Mitigation Plan Completion dated November 11, 2009, included as Attachment f-4.

g) Record Documents for CIP-007-1 R5:

i. URE's Self-Report dated June 9, 2009, included as Attachment g-1;

ii. URE's Mitigation Plan MIT-09-1889 submitted June 9, 2009, included as Attachment g-2;

iii. URE's Certification of Mitigation Plan Completion dated December 7, 2009, included as Attachment g-3; and

iv. WECC's Verification of Mitigation Plan Completion dated March 22, 2011, included as Attachment g-4.

h) Record Documents for CIP-008-1 R1:

i. URE's Self-Report dated August 12, 2008, included as Attachment h-1;

ii. URE's Mitigation Plan MIT-08-1213 submitted August 22, 2008, included as Attachment h-2;

iii. URE's Certification of Mitigation Plan Completion dated November 21, 2008, included as Attachmenth-3; and

iv. WECC's Verification of Mitigation Plan Completion dated February 19, 2009, included as Attachment h-4.

i) Disposition Document for Common Information, included as Attachment i:

i. Disposition Document for CIP-001-1 R1 and R2, included as Attachment i-1;

ii. Disposition Document for CIP-004-1 R2, included as Attachment i-2;

iii. Disposition Document for CIP-004-1 R3, included as Attachment i-3;

iv. Disposition Document for CIP-006-1 R1, included as Attachment i-4;

v. Disposition Document for CIP-007-1 R1, included as Attachment i-5;

vi. Disposition Document for CIP-007-1 R5, included as Attachment i-6;

vii. Disposition Document for CIP-008-1 R1, included as Attachment i-7;

**A Form of Notice Suitable for Publication**[11]

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

[11] *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

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.

Rebecca J. Michael*
Associate General Counsel for Corporate and Regulatory Matters
Davis Smith*
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
davis.smith@nerc.net

Mark Maher*
Chief Executive Officer
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(360) 713-9598
(801) 582-3918 – facsimile
Mark@wecc.biz

Constance White*
Vice President of Compliance
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6885
(801) 883-6894 – facsimile
CWhite@wecc.biz

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**

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*
Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Davis Smith
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
davis.smith@nerc.net

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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Attachment i

# Disposition Document for Common Information

# DISPOSITION OF VIOLATION[1]

**INFORMATION COMMON TO INSTANT VIOLATIONS**
**Dated December 10, 2010**

| REGISTERED ENTITY | NERC REGISTRY ID | NOC# |
|---|---|---|
| **Unidentified Registered Entity (URE)** | **NCRXXXXX** | **NOC-596** |

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 ☐
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 **EIGHT** VIOLATIONS OF A RELIABILITY STANDARD

(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
**URE had a documented compliance program in place at the time of the violations that WECC considered a mitigating factor in determining the penalty.**

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: **10/27/09 for CIP-001 R1-R2; CIP-004-1 R2-R3; CIP-006-1 R1; CIP-007-1 R5; and CIP-008-1 R1** OR N/A ☐

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **3/16/10** 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 ☐ NO CONTEST ☒

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-001-1 R1 and R2

# DISPOSITION OF VIOLATION
## Dated December 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **WECC200901259** | **URE_WECC20091377** |
| **WECC200901260** | **URE_WECC20091392** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-001-1** | **1** | | **Medium** | **High** |
| **CIP-001-1** | **2** | | **Medium** | **High** |

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

**The purpose statement of CIP-001-1 provides: "Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies."**

**CIP-001-1 R1 and R2 provide:**

**R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.**

**R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.**

VIOLATION DESCRIPTION

**On January 6, 2009, URE discovered and on January 9, 2009, self-reported violations of CIP-001-1 R1 and R2 to WECC, after purchasing a facility and assuming responsibility for this facility. URE stated that the facility's procedures did not define what qualifies as sabotage and how personnel are supposed to recognize sabotage, as required by R1; nor include the process for determining the appropriate parties in the Interconnection that should be notified, what information needs to be communicated, and each party's respective responsibilities, as required by R2.**

**WECC Enforcement reviewed the findings and determined that while URE had a written procedure for the recognition of sabotage events at the facility, it was not adequate for informing personnel of sabotage events, as required by R1; further, the facility's written procedures for the communication of information concerning sabotage events did not include all of the appropriate parties within the Interconnection, as required by R2.**

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

**WECC determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the facility did have some sabotage procedures in place following its registration with NERC on July 23, 2008, and the facility was disconnected from the BPS for maintenance upon purchase by URE.**

## 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) **7/23/08 through 1/16/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **1/9/09**

| | | | | |
|---|---|---|---|---|
| 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-09-1429** |
| DATE SUBMITTED TO REGIONAL ENTITY | **1/9/09 and signed 1/12/09** |
| DATE ACCEPTED BY REGIONAL ENTITY | **1/19/09** |
| DATE APPROVED BY NERC | **3/2/09** |
| DATE PROVIDED TO FERC | **3/6/09** |

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **1/16/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **1/16/09**

DATE OF CERTIFICATION LETTER **1/21/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **1/16/09**

DATE OF VERIFICATION LETTER **2/19/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **1/16/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
**To mitigate CIP-001-1 R1 and R2, URE trained all appropriate plant personnel regarding URE's sabotage reporting plan, which replaced the facility's deficient plan.**

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)
**URE's sabotage procedures were provided to the facility's personnel and sabotage training records demonstrate all appropriate personnel were trained on sabotage reporting between January 14, 2009 and January 16, 2009.**

EXHIBITS:

SOURCE DOCUMENT
**URE's Self-Reports dated January 9, 2009**

MITIGATION PLAN
**URE's Mitigation Plan MIT-09-1429 submitted January 9, 2009 and signed January 12, 2009**

CERTIFICATION BY REGISTERED ENTITY
**URE's Certification of Mitigation Plan Completion dated January 21, 2009**

VERIFICATION BY REGIONAL ENTITY
**WECC's Verification of Mitigation Plan Completion dated February 19, 2009**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-004-1 R2

# DISPOSITION OF VIOLATION
## Dated December 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **WECC200901625** | **URE_WECC20091798** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-004-1** | **2** | **2.3** | **Lower**[1] | **N/A**[2] |

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

**The purpose statement of 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 in pertinent part:**

> **R2. Training — The Responsible Entity[3] 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.**
>
> **…**

[1] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" Violation Risk Factor (VRF); R2.1, R2.2 and R2.2.4 each have a "Medium" VRF.
[2] At the time of URE's violations, CIP-004-1 had Levels of Non-Compliance instead of Violation Severity Levels (VSLs). WECC assessed a Lower VSL in the NAVAPS issued to URE based on the VSLs that had been approved by NERC, but had not yet been approved by FERC. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards; the Commission approved the VSLs on March 18, 2010.
[3] Within the text of Standard CIP-004, "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.

**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.**

**(Footnote added)**

VIOLATION DESCRIPTION

**On July 21, 2009, URE discovered, and on July 31, 2009, self-reported a violation of CIP-004-1 R2 to WECC. URE stated that one individual that had physical access to a Physical Security Perimeter (PSP) surrounding a Critical Cyber Asset location did not complete annual training by the end of the day July 18, 2009, as required by URE's Cyber Security Training Program. URE stated that it revoked this individual's access on July 21, 2009.**

**WECC subject matter experts (SMEs) reviewed URE's Self-Report and spoke with URE personnel. The SMEs found that the initial training date for the individual identified in the Self-Report was June 18, 2008. Under the URE cyber security training program, individuals must receive subsequent training regarding Critical Cyber Assets annually (defined by URE's program to be twelve months, plus or minus one month). Thus, according to URE's program, this individual must have received this training by July 18, 2009. Because this training was not performed by July 18, 2009, as required, WECC SMEs determined that URE was non-compliant.**

**WECC Enforcement reviewed the findings of the SMEs and determined that URE failed to ensure that training is conducted at least annually, as required by CIP-004-1 R2.3.**

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

**WECC determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the URE individual initially received cyber security training even though this person did not receive annual re-training in accordance with the standard. Also, URE revoked the untrained individual's authorized unescorted physical access to Critical Cyber Assets within 72 hours of the training deadline.**

## 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) **7/19/09 through 7/21/09 (date access to Critical Cyber Assets revoked)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **7/31/09**

| | | | | |
|---|---|---|---|---|
| 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-09-1993**
DATE SUBMITTED TO REGIONAL ENTITY **8/10/09**
DATE ACCEPTED BY REGIONAL ENTITY **9/10/09**
DATE APPROVED BY NERC **9/29/09**
DATE PROVIDED TO FERC **9/29/09**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **9/5/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **8/31/09**

DATE OF CERTIFICATION LETTER **9/4/09**[4]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **8/31/09**

[4] The Certification of Completion letter is dated September 2, 2009 and signed on September 4, 2009.

DATE OF VERIFICATION LETTER **11/9/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **8/31/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**To mitigate CIP-004-1 R2, URE took the following actions:**
**(1) confirmed that all personnel that currently have physical access to a PSP or logical access to a Critical Cyber Asset have completed annual training and no training expirations will occur;**
**(2) updated the cyber security training procedure to include e-mail reminders to employees in advance of training deadlines with escalation e-mails to management if training is not completed within a specified time period ahead of training deadline;**
**(3) updated the cyber security training procedure to initiate revocation by deadline of all physical and logical access to Critical Cyber Assets if training acknowledgement is not received;**
**(4) provided communication to all management of personnel that have physical access to a PSP or logical access regarding importance of performing training requirement by deadlines, immediate revocation process if training acknowledgment is not received by deadline, and accountability to ensure this is accomplished;**
**(5) implemented a design change to URE's CIP-004 tool for tracking access to Critical Cyber Assets to automatically validate that all individuals requesting logical access to Critical Cyber Assets have valid training; and**
**(6) updated the procedure for granting physical access to PSPs to validate that all individuals requesting physical access to Critical Cyber Assets have valid training through May 1, 2010.**

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)

**URE provided the following evidence in support of its completion of the Mitigation Plan:**

**(1) URE's logs demonstrating that all personnel with authorized access had completed annual training;**
**(2) URE's updated cyber security training procedure which discusses (1) e-mail reminders to employees in advance of training deadlines with escalation e-mails; and revocation by deadline of all physical and logical access to Critical Cyber Assets if training acknowledgement is not received;**

**(4) an e-mail sent to all supervisors, managers and directors of personnel with authorized access Critical Cyber Assets addressing procedures and compliance, and a log demonstrating signed acknowledgement forms;**
**(5) documentation demonstrating the new design change to URE's tool used for tracking access to Critical Cyber Assets; and**
**(6) URE's updated procedure describing the process of validating annual training that is current through a future date.**

EXHIBITS:

SOURCE DOCUMENT
**URE's Self-Report dated July 31, 2009**

MITIGATION PLAN
**URE's Mitigation Plan MIT-09-1993 submitted August 10, 2009**

CERTIFICATION BY REGISTERED ENTITY
**URE's Certification of Mitigation Plan Completion dated September 4, 2009**

VERIFICATION BY REGIONAL ENTITY
**WECC's Verification of Mitigation Plan Completion dated November 9, 2009**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-004-1 R3

# DISPOSITION OF VIOLATION
## Dated December 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **WECC200901423** | **URE_WECC20091595** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-004-1** | **3** | | **Medium**[1] | **N/A**[2] |

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

**The purpose statement of 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 R3 provides in pertinent part:**

> **R3. Personnel Risk Assessment — The Responsible Entity[3] 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**

[1] 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.

[2] At the time of URE's violations, CIP-004-1 had Levels of Non-Compliance instead of Violation Severity Levels (VSLs). WECC assessed a Severe VSL in the NAVAPS issued to URE based on the VSLs that had been approved by NERC, but had not yet been approved by FERC. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards; the Commission approved the VSLs on March 18, 2010. For this violation, WECC applied a Severe VSL because URE did not conduct its personnel risk assessments pursuant to its documented program.

[3] Within the text of Standard CIP-004, "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.

**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.**

**(Footnote added)**

VIOLATION DESCRIPTION

**On April 8, 2009, URE discovered, and on April 13, 2009, self-reported a violation of CIP-004-1 R3 to WECC.[4] URE stated that that although it had a personnel risk assessment (PRA) program, it had not followed the program with respect to 20 contract employees that had authorized access to Critical Cyber Assets. URE stated that its program required the URE Human Resource Department to perform the required assessments. Instead, URE reported that its practice has been to ask contractors to arrange for and assess the results of the identity verification and seven-year criminal background check, and then to document the results of the assessment in a letter to URE. The contractors' PRAs were completed either prior to or within 30 days of access to Critical Cyber Assets.**

**WECC subject matter experts (SMEs) reviewed URE's Self-Report and found that although URE had a PRA program and that all required PRAs were completed in a timely manner (including the PRAs for the 20 contract personnel), it was not conducting PRAs in the manner specified by its program.**

[4] URE re-submitted its Self-Report to WECC on April 23, 2009 to limit the scope of the violation to the 20 contractors.

**Enforcement reviewed the findings of the SMEs and determined that URE had a violation of CIP-004-1 R3 because it did not follow its PRA program for 20 contractors.**

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

**WECC determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because, although URE did not follow the documented process, PRAs were conducted for covered personnel such that it met the requirements of R3.1, R3.2, R3.3 and within 30 days of access being granted per R3. Additionally, although the identified URE PRAs were not performed according its internal programs in effect at the time of the violation, the URE PRA policy has since been revised to allow for this practice and were thus performed in a compliant manner.**

## 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) **7/1/08 (when the Standard became mandatory and enforceable for URE) through 4/23/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **4/13/09**

| | | | | |
|---|---|---|---|---|
| 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-09-2029**
DATE SUBMITTED TO REGIONAL ENTITY **4/23/09**
DATE ACCEPTED BY REGIONAL ENTITY **9/8/09**
DATE APPROVED BY NERC **10/13/09**
DATE PROVIDED TO FERC **10/13/09**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **4/28/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **4/23/09**

DATE OF CERTIFICATION LETTER **4/28/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **4/23/09**

DATE OF VERIFICATION LETTER **11/9/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **4/23/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
**To mitigate CIP-004-1 R3, URE took the following actions:**
**(1) updated the PRA program document to reflect the current practice relative to performing and managing PRAs for contractors/vendors; and**
**(2) communicated the updated PRA program to appropriate management.**

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)
**URE provided the following evidence in support of its completion of the Mitigation Plan:**
**(1) URE Personnel Risk Assessment program has been updated to reflect the current practice is specific to the contractor process; and**
**(2) an e-mail that communicated the updated PRA program to management.**

EXHIBITS:

SOURCE DOCUMENT
**URE's Self-Report dated April 13, 2009 and revised April 23, 2009**

MITIGATION PLAN
**URE's Mitigation Plan MIT-09-2029 submitted April 23, 2009**

CERTIFICATION BY REGISTERED ENTITY
**URE's Certification of Mitigation Plan Completion dated April 28, 2009**

VERIFICATION BY REGIONAL ENTITY
**WECC's Verification of Mitigation Plan Completion dated November 9, 2009**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-006-1 R1

# DISPOSITION OF VIOLATION
## Dated December 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **WECC200901644** | **URE_WECC20091817** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-006-1** | **1** | **1.8** | **Lower**[1] | **N/A**[2] |

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

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

**CIP-006-1 R1 provides in pertinent part:**

> **R1. Physical Security Plan — The Responsible Entity[3] 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.**

**(Footnote added)**

[1] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" Violation Risk Factor (VRF); R1.7 and R1.8 each have a "Lower" VRF. In the context of this case, WECC determined the violation related to R1.8 and therefore a "Lower" VRF is appropriate.

[2] At the time of URE's violations, CIP-006-1 had Levels of Non-Compliance instead of Violation Severity Levels (VSLs). WECC assessed a High VSL in the NAVAPS issued to URE based on the VSLs that had been approved by NERC, but had not yet been approved by FERC. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards; the Commission approved the VSLs on March 18, 2010.

[3] Within the text of Standard CIP-006, "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.

VIOLATION DESCRIPTION

**On May 26, 2009, URE discovered, and on June 30, 2009, self-reported a violation of CIP-006-1 R1 to WECC.[4] URE stated that its system for physical access control and monitoring associated with the Physical Security Perimeter (PSP) would not have in place the protective measures identified in R1.8, specifically the protective measures in CIP-005-1 and CIP-007-1, by June 30, 2009, the date that URE was required to be compliant with the Standard.**

**As to the protective measures in CIP-005-1, URE stated that the following protective measures would not be completed on time: (1) the determination of what the appropriate ports and services are for enabling and disabling per CIP-005-1 R2.2; and (2) full implementation of access point firewalls per CIP-005-1 R2.4.**

**As to the protective measures in CIP-007-1, URE stated that the following protective measures would not be completed on time: (1) the determination of what the appropriate ports and services are for enabling and disabling per CIP-007-1 R2.1 and R2.2; (2) completion of installation of malicious software prevention tools per CIP-007-1 R4.1; and (3) implementation of ability to generate user access logs of sufficient detail to create historical audit trails per CIP-007-1 R5.1.2.**

**WECC subject matter experts (SMEs) reviewed URE's Self-Report and spoke with URE personnel. The SMEs found that, at the time of the Self-Report, URE was unable to apply some of the protective measures identified in R1.8 to several Cyber Assets used in the access control and monitoring of the PSP. Specifically, WECC SMEs determined that URE was unable to apply the following protective measures:**

- **CIP-005-1 R2.2 – Enabling of only those ports necessary for normal and emergency operations,**
- **CIP-005-1 R2.4 – Ensuring authenticity of accessing party for external interactive access,**
- **CIP-007-1 R2.1 – Enabling of only those ports necessary for normal and emergency operations,**
- **CIP-007-1 R2.2 – Disabling all ports and services, including those used for testing, not needed for normal or emergency operations prior to production use of a cyber asset,**
- **CIP-007-1 R4.1 – Installation of anti-virus and malware prevention tools where technically feasible,**
- **CIP-007-1 R5.1.2 – Generating logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.**

**WECC Enforcement reviewed the findings of the SMEs and determined that URE had a violation of this CIP-006-1 R1 because it did not have in place a Physical**

[4] URE re-submitted its Self-Report to WECC on September 8, 2009 to reflect the correct FERC approved Standard.

**Security Plan with all of the protective measures for its system for physical access control and monitoring associated with the PSP, as required by R1.8.**

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

**WECC determined that the violation posed a moderate risk, but not a serious or substantial risk, because URE failed to have all of the protective measures required by CIP-005-1 and CIP-007-1 in place by June 30, 2009. Therefore, URE's access control and monitoring devices were vulnerable to compromise by an internal user. (However, the devices were protected from external users.) WECC determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because, although the devices were not extended full protection per CIP-006-1 R1.8, the risk was mitigated by the protections prescribed in CIP-004 R3, CIP-008 and CIP-009.**

## 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) **7/1/09 (when the Standard became mandatory and enforceable for URE) through 11/18/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **6/30/09**

| | | | | |
|---|---|---|---|---|
| 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-09-2015**
DATE SUBMITTED TO REGIONAL ENTITY **9/8/09**
DATE ACCEPTED BY REGIONAL ENTITY **9/9/09**
DATE APPROVED BY NERC **9/29/09**
DATE PROVIDED TO FERC **9/29/09**

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

**The Mitigation Plan was originally submitted June 30, 2009, but stated the incorrect version of the Standard, CIP-006-1a, that was not yet approved by FERC and therefore not enforceable.**

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **12/7/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **11/18/09**

DATE OF CERTIFICATION LETTER **12/7/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **11/18/09**

DATE OF VERIFICATION LETTER **6/8/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **11/18/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**To mitigate CIP-006-1 R1, URE took the following actions:**
**(1) completed the application of Anti-Virus procedures;**
**(2) installed malicious software prevention tools that fully enable or disable appropriate ports and services;**
**(3) completed the build out and verification testing of the application test server;**
**(4) finalized the initial rule set for firewalls;**
**(5) installed access point firewalls on servers;**
**(6) completed the access point firewalls;**
**(7) confirmed vendor support and finalized the contract to develop required logging;**
**(8) finalized the vendor development schedule; and**
**(9) developed the programming upgrade and implemented in production to support required logging.**

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)

**URE provided the following evidence in support of its completion of the Mitigation Plan:**
**(1) evidence that showed anti-virus protection was on Cyber Assets as of August 26, 2009;**
**(2) evidence that indicated the malicious software prevention was installed on October 9, 2009 ;**
**(3) evidence that indicated as of August 26, 2009, the set up of the application test server within the test lab was completed;**
**(4) evidence that indicated the access controls for firewalls Cyber Assets was completed on August 5, 2009;**
**(5) evidence that indicated the Cyber Assets were behind certain firewalls on September 10, 2009;**
**(6) evidence that indicated the Cyber Assets are behind certain firewalls as of September 17, 2009;**
**(7) evidence that indicated the remaining Cyber Assets are secured as of October 7, 2009;**
**(8) evidence that identifies the no additional contract was necessary for this work as it was performed and signed later using a purchase order under the original contract that URE has with its vendor;**
**(9) evidence from its vendor that showed the development schedule, scope of work and delivery date of October 21, 2009; and**
**(10) evidence that indicated access activity is now being logged as of November 18, 2009.**

EXHIBITS:

SOURCE DOCUMENT
**URE's Self-Report dated June 30, 2009 and revised September 8, 2009**

MITIGATION PLAN
**URE's Mitigation Plan MIT-09-2015 originally submitted June 30, 2009 and revised September 8, 2009**

CERTIFICATION BY REGISTERED ENTITY
**URE's Certification of Mitigation Plan Completion dated December 7, 2009**

VERIFICATION BY REGIONAL ENTITY
**WECC's Verification of Mitigation Plan Completion dated June 8, 2010**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-007-1 R1

# DISPOSITION OF VIOLATION
## Dated December 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **WECC200801706** | **URE_WECC20081880** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-007-1** | **1** | **1.2** | **Lower**[1] | **N/A**[2] |

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 a part of a group of standards numbered Standards CIP-002 through CIP-009…."**

**CIP-007-1 R1 provides in pertinent part:**

> **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.**

[1] CIP-007-1 R1 and R1.1 each have a "Medium" Violation Risk Factor (VRF); R1.2 and R1.3 each have a "Lower" VRF. In the context of this case, WECC determined the violation related to R1.2 and therefore a "Lower" VRF is appropriate.
[2] At the time of URE's violations, CIP-004-1, CIP-006-1, CIP-007-1 and CIP-008-1 had Levels of Non-Compliance instead of Violation Severity Levels (VSLs). On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards; the Commission approved the VSLs on March 18, 2010.
[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.

**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.**

**(Footnote added)**

VIOLATION DESCRIPTION

**On December 23, 2008, URE discovered, and on December 29, 2008, self-reported a violation of CIP-007-1 R1 to WECC. URE stated that it had developed test procedures for securing those systems determined to be Critical Cyber Assets, but according to these procedures, testing and documentation might not be required in some cases.**

**WECC subject matter experts (SMEs) reviewed URE's Self-Report and determined that URE had a violation of this Standard. WECC SMEs determined that this violation was the result of inconsistent testing and documentation due to confusion created by a lack of clarity and detail in URE's CIP-007-1 testing procedures. URE's testing procedures did not specify whether or not specific regression testing functions and documentation were required for certain changes. Consequently, technical personnel were not performing and documenting testing consistently.**

**WECC Enforcement reviewed the findings of the SMEs and determined that URE had a violation of CIP-007-1 R1 because it failed to have adequate test procedures and failed to perform and document testing.**

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

**WECC determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because even though there were a number of instances where tests were not executed or documented appropriately by URE, URE had conducted all other testing as required. In addition, URE's test procedures go beyond the requirements of the Standard and encompass not only the testing of significant changes that could adversely affect existing cyber security controls, but also apply to IT changes that are not related to compliance with the Standard. This violation was the result of confusion created in the procedure regarding the testing required by the Standard and the best practice production testing URE has chosen to implement above and beyond the requirements of the Standard.**

## 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) **7/1/08 (when the Standard became mandatory and enforceable for URE) through 1/30/09 (Mitigation Plan completion)**[4]

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **12/29/08**

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-08-2125**
DATE SUBMITTED TO REGIONAL ENTITY **1/8/09**
DATE ACCEPTED BY REGIONAL ENTITY **9/8/09**
DATE APPROVED BY NERC **11/12/09**
DATE PROVIDED TO FERC **11/12/09**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE
**N/A**

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **1/31/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **1/30/09**

[4] The Settlement Agreement incorrectly states that the violation duration was from December 23, 2008 until January 30, 2009.

DATE OF CERTIFICATION LETTER **2/2/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **1/30/09**

DATE OF VERIFICATION LETTER **11/11/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **1/30/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**To mitigate CIP-007-1 R1, URE took the following actions:**
**(1) provided re-training for all relevant employees;**
**(2) performed missing tests as needed and developed missing test documentation;**
**(3) developed a monthly Director review process to ensure that procedures are followed and performed the review for 6 months after development; and**
**(4) reviewed and amended its test procedures to clarify ambiguous passages and provided re-training.**

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)

**URE provided the following evidence in support of its completion of the Mitigation Plan:**
**(1) training records and materials providing a summary of what was discussed and when training was completed**
**(2) testing records for eight instances, including two re-tests demonstrating test documentation;**
**(3) process procedures showing how a supervisor will review testing and documentation to ensure procedures are understood and being implemented appropriately; and**
**(4) revised testing procedures, corresponding testing records and materials including version 2 of the modified test procedure and proof of training.**

EXHIBITS:

SOURCE DOCUMENT
**URE's Self-Report dated December 29, 2008**

MITIGATION PLAN
**URE's Mitigation Plan MIT-08-2125 submitted January 8, 2009**

CERTIFICATION BY REGISTERED ENTITY
**URE's Certification of Mitigation Plan Completion dated February 2, 2009**

VERIFICATION BY REGIONAL ENTITY
**WECC's Verification of Mitigation Plan Completion dated November 11, 2009**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-007-1 R5

# DISPOSITION OF VIOLATION
## Dated December 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **WECC200901491** | **URE_WECC20091663** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-007-1** | **5** | **5.1.2, 5.2.1** | **Medium**[1] | **N/A**[2] |

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…."**

**CIP-007-1 R5provides in pertinent part:**

> **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.**

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

[2] At the time of URE's violations, CIP-007-1 had Levels of Non-Compliance instead of Violation Severity Levels (VSLs). WECC assessed a Severe VSL in the NAVAPS issued to URE based on CIP VSLs that had been approved by NERC, but had not yet been approved by FERC. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards; the Commission approved the VSLs on March 18, 2010.

[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.

**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.**

**…**

**(Footnote added)**

VIOLATION DESCRIPTION

**On May 19, 2009, URE discovered, and on June 9, 2009, self-reported a violation of CIP-007-1 R5 to WECC. URE stated that it utilized applications and systems that could not automatically generate user access logs of sufficient detail to create historical audit trails as required by R5.1.2. In addition, URE stated that it used two Storage Area Network (SAN) systems that must remain in service and that did not allow default management accounts to be renamed or have their passwords reset per URE's policy and per R5.2.1.**

**WECC subject matter experts (SMEs) reviewed URE's Self-Report and spoke with URE personnel. WECC SMEs determined that non-compliance to R5.1.2 was due to (a) URE's application did not generate any account logging functions; (b) SAN systems did not generate any account logging functions; (c) an application for operational data did not always identify user IDs on successful login attempts and did not log failed login attempts or trust relationships; and (d) a network device could be accessed physically and manipulated without authentication prior to system configuration changes.**

**WECC SMEs also determined that non-compliance to R5.2.1 was due to SAN systems not being disabled and not being capable of password change.**

**WECC Enforcement reviewed the findings of the SMEs and determined that URE had a violation of CIP-007-1 R5 because it failed to establish methods, processes, and procedures that generate logs of sufficient detail to create audit trails of individual user account access activity for a minimum of ninety days as required by R5.1.2; and because it failed to ensure that for accounts that must remain enabled, the passwords can be changed prior to putting any system into service as required by R5.2.1.**

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

**WECC determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), but did pose a moderate risk because URE had SAN systems configured so that they could not change the passwords, thus internal users could escalate systems privileges and perform malicious acts without a record of the event. Certain of URE's applications reside within the electronic security perimeter and physical security accessible only to authorized personnel; minimizing the potential misuse by unauthorized personnel.**

## 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) **7/1/09 (when the Standard became mandatory and enforceable for URE) through 11/25/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **6/9/09**

| | | | | |
|---|---|---|---|---|
| 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-09-1889**
DATE SUBMITTED TO REGIONAL ENTITY **6/9/09**
DATE ACCEPTED BY REGIONAL ENTITY **7/20/09**
DATE APPROVED BY NERC **8/19/09**
DATE PROVIDED TO FERC **8/19/09**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE
**N/A**
MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **12/7/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **11/25/09**

DATE OF CERTIFICATION LETTER **12/7/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **11/25/09**

DATE OF VERIFICATION LETTER **3/22/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **11/25/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**To mitigate CIP-007-1 R5, URE took the following actions:**
**(1) validated NERC CIP-compliant replacements;**
**(2) purchased cyber asset replacements and upgrades;**
**(3) installed replacements and upgrades; and**
**(4) placed equipment in production and completed testing and data transfer.**

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)

**URE provided the following evidence in support of its completion of the Mitigation Plan:**

**(1) evidence to ensure compliance would or could be met by proper configuration by July 31, 2009 were reviewed.**
**(2) evidence to verify the purchase of replacements and upgrades were completed on July 23, 2009 were reviewed;**

**(3) evidence to demonstrate replacements and upgrades were installed by September 29, 2009 were reviewed; and**
**(4) evidence to demonstrate equipment was placed in production and testing and data migration to the new system was completed on November 25, 2009 were reviewed.**

EXHIBITS:

SOURCE DOCUMENT
**URE's Self-Report dated June 9, 2009**

MITIGATION PLAN
**URE's Mitigation Plan MIT-09-1889 submitted June 9, 2009**

CERTIFICATION BY REGISTERED ENTITY
**URE's Certification of Mitigation Plan Completion dated December 7, 2009**

VERIFICATION BY REGIONAL ENTITY
**WECC's Verification of Mitigation Plan Completion dated March 22, 2011**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-008-1 R1

# DISPOSITION OF VIOLATION
## Dated December 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **WECC200801185** | **URE_WECC20081293** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-008-1** | **1** | **1.3** | **Lower** | **N/A**[1] |

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

**The purpose statement of CIP-008-1 provides in pertinent part: "Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."**

**CIP-008-1 R1 provides in pertinent part:**

> **R1. Cyber Security Incident Response Plan — The Responsible Entity[2] shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:**
>
> > **R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.**
> >
> > **R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.**
> >
> > **R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC).**

[1] At the time of URE's violations, CIP-008-1 had Levels of Non-Compliance instead of Violation Severity Levels (VSLs). WECC assessed a High VSL in the NAVAPS issued to URE based on CIP VSLs that had been approved by NERC, but had not yet been approved by FERC. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards; the Commission approved the VSLs on March 18, 2010.

[2] Within the text of Standard CIP-008, "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.

**The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.**

**…**
**(Footnote added)**

VIOLATION DESCRIPTION

**On August 4, 2008, URE discovered, and on August 12, 2008, self-reported a violation of CIP-008-1 R1 to WECC. URE stated that on July 28, 2008 through July 29, 2008 because of an equipment failure, URE's control center lost Supervisory Control and Data Acquisition (SCADA) for some time certain. URE stated that this event should have triggered the initiation of its Cyber Security Incident response plan and a report to ES ISAC, as required by R1.3. However, URE did not initiate the plan and thereby did not make the appropriate notification to ES ISAC.**

**Enforcement reviewed the previous findings and determined that URE had a violation of CIP-008-1 R1 because it failed to ensure that a reportable Cyber Security Incident was reported to ES ISAC either directly or through an intermediary, as required by R1.3.**

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

**WECC determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because URE had a Cyber Security Incident response plan with the required elements. Although URE did not report the Cyber Security Incident to ES-ISAC pursuant to its plan, URE did identify, classify and respond to the Incident. Further, the incident, a failure of SCADA, WECC determined that URE's failure to follow its Cyber Security Incident response plan and report an incident to ES ISAC, did not result in a breach to URE's cyber security or threaten the reliability of the BPS.**

## 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) **7/28/08 (the date of the reportable Cyber Security Incident) through 11/20/08 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **8/12/08**

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-08-1213**
DATE SUBMITTED TO REGIONAL ENTITY **8/22/08**
DATE ACCEPTED BY REGIONAL ENTITY **8/26/08**
DATE APPROVED BY NERC **1/6/09**
DATE PROVIDED TO FERC **1/6/09**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE
**N/A**
MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **11/23/08**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **11/20/08**

DATE OF CERTIFICATION LETTER **11/21/08**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **11/20/08**

DATE OF VERIFICATION LETTER **2/19/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **11/20/08**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**To mitigate CIP-008-1 R1, URE took the following actions:**

**(1) sent notice to all pertinent personnel reminding them of incident communication requirements;**
**(2) completed a root cause analysis of the incident;**

**(3) update its Cyber Security Incident response plan with lessons learned; and**
**(4) completed training of appropriate personnel for communication and incident response plans.**

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)

**URE provided the following evidence in support of its completion of the Mitigation Plan:**

**(1) the internal communication sent to remind personnel of incident communication requirements;**
**(2) URE's root cause analysis;**
**(3) URE's updated Cyber Security Incident response plan, summary of changes and lessons learned; and**
**(4) URE's communication and incident response plan training records.**

EXHIBITS:

SOURCE DOCUMENT
**URE's Self-Report dated August 12, 2008**

MITIGATION PLAN
**URE's Mitigation Plan MIT-08-1213 submitted August 22, 2008**

CERTIFICATION BY REGISTERED ENTITY
**URE's Certification of Mitigation Plan Completion dated November 21, 2008**

VERIFICATION BY REGIONAL ENTITY
**WECC's Verification of Mitigation Plan Completion dated February 19, 2009**