



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 violation<sup>1</sup> discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Documents (Attachment n), 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)).<sup>2</sup>

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-003-1 Requirement (R) 1/1.1, CIP-006-1 R1/1.8 and CIP-007-1 R1/1.1. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of thirteen thousand dollars (\$13,000), in addition to other remedies and actions to mitigate the

<sup>1</sup> 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.

<sup>2</sup> *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).

instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC200901677, WECC200901678 and WECC200901679 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 May 24, 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-566	WECC200901677	CIP-003-1	1/1.1	Lower <sup>3</sup>	7/1/08-6/22/09	13,000
	WECC200901678	CIP-006-1	1/1.8	Lower <sup>4</sup>	7/1/09-11/20/09	
	WECC200901679	CIP-007-1	1/1.1	Medium <sup>5</sup>	7/1/08-11/15/09	

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

<sup>3</sup> When NERC filed Violation Risk Factors (VRF) it originally assigned CIP-003-1 R1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-003-1 R1 was in effect from June 18, 2007 until January 27, 2009 when the "Medium" VRF became effective. CIP-003-1R1.1, R1.2 and R1.3 each have a "Lower" VRF. In the context of this case, WECC determined that the violation related to R1.1, and therefore a "Lower" VRF is appropriate.

<sup>4</sup> When NERC filed VRFs it originally assigned CIP-006-1 R1.5 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on February 2, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-006-1 R1.5 was in effect from June 18, 2007 until February 2, 2009 when the "Medium" VRF became effective. CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, and R1.6 each have a "Medium" VRF; R1.7, R1.8 and R1.9 each have a "Lower" VRF. In the context of this case, WECC determined that the violation related to R1.8, and therefore a "Lower" VRF is appropriate.

<sup>5</sup> When NERC filed VRFs it originally assigned CIP-007-1 R1.1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-007-1 R1.1 was in effect from June 18, 2007 until January 27, 2009 when the "Medium" VRF became effective. CIP-007-1 R1 has a "Medium" VRF and CIP-007-1 R1.2 and R1.3 each have a "Lower" VRF.

#### CIP-003-1 R1/1.1 - OVERVIEW

During a Spot Check, WECC discovered a violation of CIP-003-1 R1/1.1. WECC determined that URE did not document and implement a cyber security policy that addressed all of the requirements in CIP-002 through CIP-009, specifically the CIP-004 R1 requirement to establish, maintain and document a security awareness program to ensure that personnel having authorized access to Critical Cyber Assets receive on-going reinforcement in sound security practices.

#### CIP-006-1 R1/1.8 - OVERVIEW

During a Spot Check, WECC discovered a violation of CIP-006-1 R1/1.8. WECC determined that URE did not exercise, at least annually, recovery plans as specified in CIP-009 R2, for Cyber Assets used in the access control and monitoring of the Physical Security Perimeter.

#### CIP-007-1 R1/1.1 - OVERVIEW

During a Spot Check, WECC discovered a violation of CIP-007-1 R1/1.1. WECC determined that URE did not have adequate cyber security test procedures specifically ensuring that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls.

### **Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed<sup>6</sup>**

#### **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,<sup>7</sup> the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on November 2, 2010. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a thirteen thousand dollar (\$13,000) 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:<sup>8</sup>

1. the violations constituted URE's first violation of the subject NERC Reliability Standards;
2. WECC reported that URE was cooperative throughout the compliance enforcement process;

<sup>6</sup> See 18 C.F.R. § 39.7(d)(4).

<sup>7</sup> *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).

<sup>8</sup> URE did not receive credit for having a compliance program because it was not reviewed by WECC at the time of the violations.

3. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
4. 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
5. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement. The NERC BOTCC agreed that the assessed penalty of thirteen thousand dollars (\$13,000) 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.

### **Request for Confidential Treatment**

Information in and certain attachments to the instant Notice of Penalty include privileged and 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. Specifically, this includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business and confidential information exempt from the mandatory public disclosure requirements of the Freedom of Information Act, 5 U.S.C. 552, and should be withheld from public disclosure.

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 May 24, 2010, included as Attachment a;
- b) WECC's Determination of Alleged Violation Summary for CIP-003-1 R1, included as Attachment b;

- c) WECC's Determination of Alleged Violation Summary for CIP-006-1 R1, included as Attachment c;<sup>9</sup>
- d) WECC's Determination of Alleged Violation Summary for CIP-007-1 R1, included as Attachment d;<sup>10</sup>
- e) URE's Mitigation Plan for CIP-003-1 R1 designated as MIT-08-2228 submitted December 1, 2009, included as Attachment e;
- f) URE's Certification of Mitigation Plan Completion for CIP-003-1 R1 dated December 1, 2009, included as Attachment f;
- g) WECC's Verification of Mitigation Plan Completion for CIP-003-1 R1 dated December 31, 2009, included as Attachment g;
- h) URE's Mitigation Plan for CIP-006-1 R1 designated as MIT-09-2264 dated November 23, 2009, included as Attachment h;
- i) URE's Certification of Mitigation Plan Completion for CIP-006-1 dated November 23, 2009, included as Attachment i;
- j) WECC's Verification of Mitigation Plan Completion for CIP-006-1 R1 dated February 9, 2010, included as Attachment j;
- k) URE's Mitigation Plan for CIP-007-1 R1 designated as MIT-08-2265 dated November 23, 2009, included as Attachment k;
- l) URE's Certification of Mitigation Plan Completion for CIP-007-1 R1 dated November 23, 2009, included as Attachment l;
- m) WECC's Verification of Mitigation Plan Completion for CIP-007-1 R1 dated February 9, 2010, included as Attachment m;
- n) Disposition Document for Common Information, included as Attachment n:
  - i. Disposition Document for CIP-003-1 R1, included as Attachment n-1;
  - ii. Disposition Document for CIP-006-1 R1, included as Attachment n-2;
  - iii. Disposition Document for CIP-007-1 R1, included as Attachment n-3;

### **A Form of Notice Suitable for Publication<sup>11</sup>**

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

---

<sup>9</sup> The Determination of Alleged Violation Summary document incorrectly states that the Mitigation Plan was submitted on November 25, 2009.

<sup>10</sup> *Id.*

<sup>11</sup> *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:

<p>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</p> <p>Christopher Luras* Manager of Compliance Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz</p> <p>*Persons to be included on the Commission’s service list are indicated with an asterisk. NERC requests waiver of the Commission’s rules and regulations to permit the inclusion of more than two people on the service list.</p>	<p>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</p> <p>Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 713-9598 (801) 582-3918 – facsimile Mark@wecc.biz</p> <p>Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6885 (801) 883-6894 – facsimile CWhite@wecc.biz</p> <p>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</p>
--	--

## Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Abbreviated NOP as compliant with its rules, regulations and orders.

Respectfully submitted,

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

/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

cc: Unidentified Registered Entity  
Western Electricity Coordinating Council

Attachments

## **Attachment n**

# **Disposition Document for Common Information**



**DISPOSITION OF VIOLATION<sup>1</sup>**  
**INFORMATION COMMON TO INSTANT VIOLATIONS**  
**Dated November 30, 2010**

REGISTERED ENTITY                      NERC REGISTRY ID                      NOC#  
**Unidentified Registered Entity**      **NCRXXXXX**                      **NOC-566**  
**(URE)**

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 **\$13,000** FOR **THREE (3)**  
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

---

<sup>1</sup> 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 did not receive credit for having a compliance program because  
it was not reviewed by WECC at the time of the 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

Attachment n

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

(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: **11/3/09** OR N/A

SETTLEMENT DISCUSSIONS COMMENCED

DATE: **2/9/10** 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

## **Disposition Document for CIP-003-1 R1**

## **DISPOSITION OF VIOLATION**

**Dated November 30, 2010**

NERC TRACKING NO. <b>WECC200901677</b>	REGIONAL ENTITY TRACKING NO. <b>URE_WECC20091850</b>
---	---

### **I. VIOLATION INFORMATION**

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
<b>CIP-003-1</b>	<b>1</b>	<b>1.1</b>	<b>Lower<sup>1</sup></b>	<b>N/A</b>

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

**The purpose statement of CIP-003-1 provides in pertinent part: “Standard CIP-003 requires that Responsible Entities<sup>[2]</sup> have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009....” (Footnote added.)**

**CIP-003-1 R1 provides:**

**R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management’s commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:**

**R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.**

---

<sup>1</sup> When NERC filed Violation Risk Factors (VRF) it originally assigned CIP-003-1 R1 a “Lower” VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified “Medium” VRF and on January 27, 2009, the Commission approved the modified “Medium” VRF. Therefore, the “Lower” VRF for CIP-003-1 R1 was in effect from June 18, 2007 until January 27, 2009 when the “Medium” VRF became effective. CIP-003-1 R1.1, R1.2 and R1.3 each have a “Lower” VRF. In the context of this case, WECC determined that the violation related to R1.1, and therefore a “Lower” VRF is appropriate.

<sup>2</sup> Within the text of Standard CIP-003, “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**

**WECC conducted a CIP Spot Check of URE. During the course of its investigation, WECC discovered a violation of CIP-003-1 R1/1.1. WECC subject matter experts (SMEs) reviewed two URE cyber security policies.**

**The SMEs found that the first cyber security policy addressed all the requirements in CIP-002 through CIP-009 except for CIP-004 R1 regarding establishment of a security awareness program. The SMEs found that the later dated cyber security policy, addressed all of the requirements in CIP-002 through CIP-009 including CIP-004 R1.**

**Enforcement reviewed the findings of the SMEs and determined that URE had a violation of this Standard because it failed to document and implement a cyber security policy that addressed the requirement in CIP-004 R1 to establish, maintain and document a security awareness program to ensure that personnel having authorized access to Critical Cyber Assets receive on-going reinforcement in sound security practices.**

**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 was not required to be compliant with CIP-004 R1 and establish and maintain a security awareness program until a certain date. WECC determined that URE's noncompliance did not pose a significant risk.<sup>3</sup>**

**II. DISCOVERY INFORMATION**

**METHOD OF DISCOVERY**

- |                                    |                                     |
|------------------------------------|-------------------------------------|
| SELF-REPORT                        | <input type="checkbox"/>            |
| SELF-CERTIFICATION                 | <input type="checkbox"/>            |
| COMPLIANCE AUDIT                   | <input type="checkbox"/>            |
| COMPLIANCE VIOLATION INVESTIGATION | <input type="checkbox"/>            |
| SPOT CHECK                         | <input checked="" type="checkbox"/> |
| COMPLAINT                          | <input type="checkbox"/>            |
| PERIODIC DATA SUBMITTAL            | <input type="checkbox"/>            |
| EXCEPTION REPORTING                | <input type="checkbox"/>            |

**DURATION DATE(S) 7/1/08 (when the Standard became mandatory and enforceable for URE) through 6/23/09 (Mitigation Plan completion)**

**DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY Spot Check**

---

<sup>3</sup> The Settlement Agreement states that the risk to the BPS is minimal and Spot Check document states that the risk to the BPS is moderate.

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

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-08-2228**  
DATE SUBMITTED TO REGIONAL ENTITY    **12/1/09**  
DATE ACCEPTED BY REGIONAL ENTITY    **12/18/09**  
DATE APPROVED BY NERC    **1/6/10**  
DATE PROVIDED TO FERC    **1/6/10**

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

N/A

MITIGATION PLAN COMPLETED      YES       NO

EXPECTED COMPLETION DATE **Submitted as complete**  
EXTENSIONS GRANTED      **N/A**  
ACTUAL COMPLETION DATE    **6/23/09**

DATE OF CERTIFICATION LETTER **12/1/09**  
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **6/23/09**

DATE OF VERIFICATION LETTER **12/31/09**  
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **6/23/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**To mitigate CIP-003-1 R1/1.1, URE stated that it had already implemented a cyber security policy that adequately addressed a security awareness program.**

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 two cyber security policy documents that were in effect during the audit period.**

EXHIBITS:

SOURCE DOCUMENT

**WECC's Determination of Alleged Violation Summary for CIP-003-1 R1**

MITIGATION PLAN

**URE's Mitigation Plan for CIP-003-1 R1 designated as MIT-08-2228  
submitted December 1, 2009**

CERTIFICATION BY REGISTERED ENTITY

**URE's Certification of Mitigation Plan Completion for CIP-003-1 R1 dated  
December 1, 2009**

VERIFICATION BY REGIONAL ENTITY

**WECC's Verification of Mitigation Plan Completion for CIP-003-1 R1 dated  
December 31, 2009**



## **Disposition Document for CIP-006-1 R1**

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

## **DISPOSITION OF VIOLATION**

**Dated November 2, 2010**

NERC TRACKING NO. WECC200901678	REGIONAL ENTITY TRACKING NO. URE_WECC20091851
---------------------------------------	---

### **I. VIOLATION INFORMATION**

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
<b>CIP-006-1</b>	<b>1</b>	<b>1.8</b>	<b>Lower<sup>1</sup></b>	<b>N/A</b>

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<sup>[2]</sup> 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.)**

<sup>1</sup> When NERC filed VRFs it originally assigned CIP-006-1 R1.5 a “Lower” VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified “Medium” VRF and on February 2, 2009, the Commission approved the modified “Medium” VRF. Therefore, the “Lower” VRF for CIP-006-1 R1.5 was in effect from June 18, 2007 until February 2, 2009 when the “Medium” VRF became effective. CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, and R1.6 each have a “Medium” Violation Risk Factor (VRF); R1.7, R1.8 and R1.9 each have a “Lower” VRF. In the context of this case, WECC determined that the violation related to R1.8, and therefore a “Lower” VRF is appropriate.

<sup>2</sup> 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.

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

**VIOLATION DESCRIPTION**

**During a Spot Check, WECC discovered a violation of CIP-006-1 R1/1.8. During the course of the investigation, URE provided a copy of its current recovery plan for Cyber Assets used in the access control and monitoring of the Physical Security Perimeter. WECC subject matter experts (SMEs) reviewed the documentation provided by URE and determined that Cyber Assets used in the access control and monitoring of the Physical Security Perimeter were not afforded protective measures required under CIP-006-1 R1.8 and specified by CIP-009 R2.**

**Enforcement reviewed the findings of the SMEs and determined that URE had a violation of this Standard because it failed to exercise, at least annually, recovery plans for Cyber Assets used in the access control and monitoring of the Physical Security Perimeter.**

**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 did have a recovery plan for the applicable Cyber Assets. However, WECC determined that a failure to exercise at least annually the recovery plans for Cyber Assets used in the access control and monitoring of the Physical Security Perimeter could reduce the speed with which such assets could be recovered in the event of loss. This could result in an increase risk of unauthorized access to the Physical Security Perimeters and an increased risk of authorized access to the Physical Security Perimeters would not be readily available.**

**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 11/20/09 (Mitigation Plan completion)**

**DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY Spot Check**  
**IS THE VIOLATION STILL OCCURRING YES  NO**   
**IF YES, EXPLAIN**

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

REMEDIAL ACTION DIRECTIVE ISSUED	YES	<input type="checkbox"/>	NO	<input checked="" type="checkbox"/>
PRE TO POST JUNE 18, 2007 VIOLATION	YES	<input type="checkbox"/>	NO	<input checked="" type="checkbox"/>

### **III. MITIGATION INFORMATION**

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	<b>MIT-09-2264</b>
DATE SUBMITTED TO REGIONAL ENTITY	<b>11/25/09</b>
DATE ACCEPTED BY REGIONAL ENTITY	<b>1/5/10</b>
DATE APPROVED BY NERC	<b>1/19/10</b>
DATE PROVIDED TO FERC	<b>1/21/10</b>

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

N/A

MITIGATION PLAN COMPLETED      YES       NO

EXPECTED COMPLETION DATE	<b>Submitted as complete</b>
EXTENSIONS GRANTED	<b>N/A</b>
ACTUAL COMPLETION DATE	<b>11/20/09</b>

DATE OF CERTIFICATION LETTER **11/25/09**  
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **11/20/09**

DATE OF VERIFICATION LETTER **2/9/10**  
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **11/20/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**To mitigate CIP-006-1 R1/1.8, URE completed an exercise of the recovery plan for Cyber Assets used in the access control and monitoring of the Physical Security Perimeter.**

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 a copy of its recovery plan and the recovery plan exercise to WECC.**

EXHIBITS:

SOURCE DOCUMENT

**WECC's Determination of Alleged Violation Summary for CIP-006-1 R1**

MITIGATION PLAN

**URE's Mitigation Plan for CIP-006-1 R1 designated as MIT-09-2264 dated November 23, 2009 and submitted November 25, 2009**

CERTIFICATION BY REGISTERED ENTITY

**URE's Certification of Mitigation Plan Completion for CIP-006-1 R1 dated November 23, 2009 and submitted November 25, 2009**

VERIFICATION BY REGIONAL ENTITY

**WECC's Verification of Mitigation Plan Completion for CIP-006-1 R1 dated February 9, 2010**

## **Disposition Document for CIP-007-1 R1**

## **DISPOSITION OF VIOLATION**

**Dated November 2, 2010**

NERC TRACKING NO. <b>WECC200901679</b>	REGIONAL ENTITY TRACKING NO. <b>URE_WECC20091852</b>
---	---

### **I. VIOLATION INFORMATION**

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
<b>CIP-007-1</b>	<b>1</b>	<b>1.1</b>	<b>Medium<sup>1</sup></b>	<b>N/A</b>

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: “Standard CIP-007 requires Responsible Entities<sup>[2]</sup> 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 R1 provides:**

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

---

<sup>1</sup> When NERC filed VRFs it originally assigned CIP-007-1 R1.1 a “Lower” VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified “Medium” VRF and on January 27, 2009, the Commission approved the modified “Medium” VRF. Therefore, the “Lower” VRF for CIP-007-1 R1.1 was in effect from June 18, 2007 until January 27, 2009 when the “Medium” VRF became effective. CIP-007-1 R1 has a “Medium” VRF and CIP-007-1 R1.2 and R1.3 each have a “Lower” VRF.

<sup>2</sup> 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.

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

**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.**

**VIOLATION DESCRIPTION**

**During a Spot Check, WECC discovered a violation of CIP-007-1 R1/1.1. WECC subject matter experts (SMEs) reviewed the documentation provided by URE to demonstrate compliance with this Standard. After thorough review, WECC determined that the documents did not contain test procedures specifically ensuring that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. Rather, the SMEs determined that the documentation provided by URE focused on testing functionality of the system and not existing cyber security controls.**

**Enforcement reviewed the findings of the SMEs and determined that URE had a violation of this Standard because it failed to have cyber security test procedures that 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.**

**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 did present sufficient evidence to demonstrate that the test procedures would minimize adverse effects on the system and its operations. Nevertheless, WECC determined that the violation posed a moderate risk because URE’s failure to create and implement cyber security test procedures could result in system compromise.**

**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 11/15/09 (Mitigation Plan completion)**



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

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **Spot Check**  
**Date**

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-08-2265**  
DATE SUBMITTED TO REGIONAL ENTITY    **11/25/09**  
DATE ACCEPTED BY REGIONAL ENTITY    **1/5/10**  
DATE APPROVED BY NERC    **1/19/10**  
DATE PROVIDED TO FERC    **1/21/10**

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

**N/A**

MITIGATION PLAN COMPLETED      YES       NO

EXPECTED COMPLETION DATE **Submitted as complete**  
EXTENSIONS GRANTED      **N/A**  
ACTUAL COMPLETION DATE    **11/15/09**

DATE OF CERTIFICATION LETTER **11/25/09**  
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **11/15/09**

DATE OF VERIFICATION LETTER **2/9/10**  
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **11/15/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT  
RECURRENCE

**To mitigate CIP-007-1 R1/1.1, URE modified its cyber security testing  
program to include procedures for evaluating the impact of installing new or  
significantly changed assets within the Electronic Security Perimeter.**

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

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 its Cyber Security controls testing procedure**

EXHIBITS:

SOURCE DOCUMENT

**WECC's Determination of Alleged Violation Summary**

MITIGATION PLAN

**URE's Mitigation Plan for CIP-007-1 R1 designated as MIT-08-2265 dated  
November 23, 2009**

CERTIFICATION BY REGISTERED ENTITY

**URE's Certification of Mitigation Plan Completion for CIP-007-1 R1 dated  
November 23, 2009**

VERIFICATION BY REGIONAL ENTITY

**WECC's Verification of Mitigation Plan Completion**