



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 violation¹ discussed in detail in the Disposition Documents attached hereto (Attachment a), 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

During a Spot Check, the Western Electricity Coordinating Council (WECC) identified violations of Reliability Standards CIP-002-1 Requirement (R) 2 and CIP-008-1 R1 for URE's failure to properly update its list of Critical Assets and failure to include a process for ensuring annual testing in its Cyber Security incident response plan. On September 8, 2009 and again on October 20, 2009, URE self-reported a violation of CIP-007-1 R6/6.5 to WECC for URE's failure to review logs of system events related to cyber security to support incident response and maintain records documenting its review of the logs. This NOP is being filed with the Commission because URE does not dispute the violations of CIP-002-1 R2, CIP-007-1 R6 and CIP-008-1 R1 and the assessed fourteen thousand five hundred dollar (\$14,500) penalty. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers

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).

NERC Abbreviated Notice of Penalty Unidentified Registered Entity HAS BEEN REMOVED FROM THIS PUBLIC VERSION
 March 30, 2011

Page 2

WECC200901642, WECC200901698 and WECC200901643 are Confirmed Violations, as that term is defined in 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 Notice of Confirmed Violation and Proposed Penalty or Sanction (NOCV). 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 this NOP by the NERC Board of Trustees Compliance Committee (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 at issue in this NOP.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty (\$)
WECC	Unidentified Registered Entity	NOC-435	WECC200901642	CIP-002-1	2	High ³	\$14,500
			WECC200901698	CIP-007-1	6/6.5	Lower ⁴	
			WECC200901643	CIP-008-1	1 ⁵ /1.6	Lower	

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed⁶

Basis for Determination

Taking into consideration the Commission’s direction in Order No. 693, the NERC Sanction Guidelines and the Commission’s July 3, 2008 and October 26, 2009 Guidance Orders,⁷ the NERC BOTCC reviewed the NOCV and supporting documentation on July 12, 2010. The

³ When NERC filed Violation Risk Factors (VRF) it originally assigned CIP-002-1 R2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on January 27, 2009, the Commission approved the modified High VRF. Therefore, the Lower VRF for CIP-002-1 R2 was in effect from June 18, 2007 until January 27, 2009 when the High VRF became effective. The source document incorrectly states a “Lower” VRF.

⁴ When NERC filed VRFs it originally assigned CIP-007-1 R6.1, R6.2 and R6.3 Lowers VRF. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on February 2, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-007-1 R6.1, R6.2 and R6.3 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective. CIP-007-1 R6, R6.4 and R6.5 each have a “Lower” VRF; R6.1, R6.2 and R6.3 each have a “Medium” VRF.

⁵ CIP-008-1 R1 became mandatory and enforceable for System Control Center Balancing Authorities and Transmission Operators functions on July 1, 2008 and for other facilities’ Balancing Authorities and Transmission Operators functions on July 1, 2009.

⁶ See 18 C.F.R § 39.7(d)(4).

⁷ *North American Electric Reliability Corporation*, “Guidance Order on Reliability Notices of Penalty,” 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, “Further Guidance Order on Reliability Notices of Penalty,” 129 FERC ¶ 61,069 (2009). See also *North American Electric Reliability Corporation*, “Notice of No Further Review and Guidance Order,” 132 FERC ¶ 61,182 (2010).

NERC BOTCC approved the NOCV and the assessment of a fourteen thousand five hundred dollar (\$14,500) financial penalty against URE based upon WECC's findings and determinations, the NERC BOTCC's review of 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. the violations of CIP-002-1 R2 and CIP-007-1 R6 constituted URE's first occurrence of violations of the subject NERC Reliability Standards;
2. the violation of CIP-008-1 R1 was a second violation;
3. URE self-reported the violation of CIP-007-1 R6;
4. WECC reported that URE was cooperative throughout the compliance enforcement process;
5. URE has a compliance program, which WECC considered to be a neutral factor in the penalty determination, as discussed in the Disposition Documents;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violations did not pose a serious or substantial risk to the BPS, as discussed in the Disposition Documents; and
8. 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 believes that the assessed penalty of fourteen thousand five hundred dollars (\$14,500) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the bulk power system.

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 the Commission, or, if the Commission decides to review the penalty, upon final determination by the Commission.

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) Disposition Document for Common Information dated July 12, 2010, included as Attachment a;
 - a. Disposition Document for CIP-002-1 R2, included as Attachment a-1;
 - b. Disposition Document for CIP-007-1 R6, included as Attachment a-2;
 - c. Disposition Document for CIP-008-1 R1, included as Attachment a-3;
- b) URE's Response to the Notice of Alleged Violation and Proposed Penalty or Sanction dated December 3, 2009, included as Attachment b;
- c) Record documents for CIP-002-1 R2 included as Attachment c:
 - a. WECC's Spot Check Screen Shot;
 - b. URE's Mitigation Plan designated as MIT-08-2229 dated December 1, 2009;
 - c. URE's Certification of Mitigation Plan Completion dated December 1, 2009;
 - d. WECC's Verification of Mitigation Plan Completion dated December 31, 2009;
- d) Record documents for CIP-007-1 R6 included as Attachment d:
 - a. URE's Self-Report dated October 20, 2009;
 - b. URE's Mitigation Plan designated as MIT-09-2072 submitted on October 20, 2009;
 - c. URE's Certification of Mitigation Plan Completion dated October 28, 2009;⁸
 - d. WECC's Verification of Mitigation Plan Completion dated December 2, 2009;
- e) Record documents for CIP-008-1 R1 included as Attachment e:
 - a. WECC's Spot Check Screen Shot;
 - b. URE's Mitigation Plan designated as MIT-09-2374 dated July 24, 2009;
 - c. URE's Certification of Mitigation Plan Completion dated July 24, 2009; and
 - d. WECC's Verification of Mitigation Plan Completion dated March 8, 2010.

A Form of Notice Suitable for Publication⁹

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

⁸ The Certification of Completion document is dated October 27, 2009.

⁹ 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</p> <p>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</p> <p>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) 883-6855 (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>
---	---

NERC Abbreviated Notice of Penalty Unidentified Registered Entity
March 30, 2011
Page 7

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this 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 a

Disposition Document for Common Information dated July 12, 2010

PRIOR VIOLATIONS OF OTHER RELIABILITY STANDARD(S) OR
REQUIREMENTS THEREUNDER

YES NO

LIST ANY PRIOR CONFIRMED OR SETTLED 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
EXPLAIN

**WECC reviewed URE's ICP and considered the ICP to be a neutral
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.

See above.

(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: **11/17/2009** OR N/A

SETTLEMENT DISCUSSIONS COMMENCED

DATE: OR N/A

NOTICE OF CONFIRMED VIOLATION ISSUED

DATE: **12/10/2009** 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-002-1 R2

DISPOSITION OF VIOLATION
Dated July 12, 2010

NERC TRACKING NO. WECC200901642 REGIONAL ENTITY TRACKING NO. URE_WECC20091815

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-002-1	2		High ¹	Severe

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

The purpose statement of CIP-002-1 provides in pertinent part: “... Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.”

CIP-002-1 R2 provides: “Critical Asset Identification – The Responsible Entity^[2] shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.” (Footnote added.)

VIOLATION DESCRIPTION

During a Spot Check conducted by WECC, WECC discovered that URE owns a substation, which URE failed to include as a Critical Asset based on its risk-based methodology.

URE had a list of Critical Assets dated June 2008 and a revised list of Critical Assets dated June 2009. URE had removed facilities from its 2008 list of Critical Assets based on a revised assessment of whether they were Critical Facilities. WECC

¹ When NERC filed Violation Risk Factors (VRF) it originally assigned CIP-002-1 R2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on January 27, 2009, the Commission approved the modified High VRF. Therefore, the Lower VRF for CIP-002-1 R2 was in effect from June 18, 2007 until January 27, 2009 when the High VRF became effective. The source document incorrectly states a “Lower” VRF.

² Within the text of Standard CIP-002, “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.

reviewed the facilities using URE’s revised risk-based methodology and determined that a substation was a Critical Asset under URE’s revised risk-based assessment methodology. Based on this determination, WECC concluded the substation should not have been removed from the list of URE’s Critical Assets and therefore, URE had a violation of CIP-002-1 R2 for its failure to properly update its list of Critical Assets.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Although WECC determined the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), WECC determined it was moderate because the substation was not included on URE’s list of Critical Assets for approximately six (6) months. Because URE did not include the Substation on its list of Critical Assets, it was not identified as requiring the consideration and protection afforded to Critical Assets per the other CIP Reliability Standards. Critical Assets often rely on each other, across functions and organizations, for services and data critical to the operation of the BES. Therefore there was an increased risk to all of URE’s Critical Assets vital to the operation of the BES.

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) **approximately six (6) months**

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-08-2229**
DATE SUBMITTED TO REGIONAL ENTITY **12/1/2009**
DATE ACCEPTED BY REGIONAL ENTITY **12/22/2009**
DATE APPROVED BY NERC **1/5/2010**
DATE PROVIDED TO FERC **1/5/2010**

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

URE initially submitted a Mitigation Plan to WECC on November 6, 2009. URE submitted a revised Mitigation Plan on December 1, 2009 (as shown above).

MITIGATION PLAN COMPLETED YES NO

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **11/22/2009**

DATE OF CERTIFICATION LETTER **12/1/2009**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **11/22/2009**

DATE OF VERIFICATION LETTER **12/31/2009**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **11/22/2009**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE updated its list of Critical Assets to include a substation.

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 submitted its revised Critical Asset List dated November 22, 2009.

EXHIBITS (SEE ATTACHMENTS TO NOTICE OF PENALTY):

SOURCE DOCUMENT

WECC's Spot Check Screen Shot

MITIGATION PLAN

Mitigation Plan designated as MIT-08-2229 dated December 1, 2009

CERTIFICATION BY REGISTERED ENTITY

Certification of Mitigation Plan Completion (contained within the Mitigation Plan) dated December 1, 2009

VERIFICATION BY REGIONAL ENTITY

Verification of Mitigation Plan Completion dated December 31, 2009

Disposition Document for CIP-007-1 R6

DISPOSITION OF VIOLATION
Dated July 12, 2010

NERC TRACKING NO. WECC200901698 REGIONAL ENTITY TRACKING NO. URE_WECC20091872

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	6	6.5	Lower ¹	Severe

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^[2] 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 R6 provides in pertinent part:

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

...

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

¹ When NERC filed VRFs it originally assigned CIP-007-1 R6.1, R6.2 and R6.3 Lowers VRF. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on February 2, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-007-1 R6.1, R6.2 and R6.3 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective. CIP-007-1 R6, R6.4 and R6.5 each have a “Lower” VRF; R6.1, R6.2 and R6.3 each have a “Medium” VRF.

² 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.

VIOLATION DESCRIPTION

During a CIP compliance self-assessment conducted by URE compliance personnel, URE discovered a violation of CIP-007-1 R6. On September 8, 2009, URE self-reported a violation of CIP-007-1 R6, specifically R6.5. URE submitted a revised Self-Report on October 20, 2009. URE reported that it had not reviewed logs of system events related to cyber security, nor had it maintained records documenting its review of the logs, as required by R6.5. A WECC subject matter expert confirmed that URE was producing the security logs, but did not review them from July 1, 2009 to August 28, 2009.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Although WECC determined the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), WECC determined it was moderate because URE did not review the logs for two months and therefore, would have been unable to identify and react to security events that might have been indicators of a cyber security attack. As a result of this lack of cyber security log review, URE exposed its Critical Cyber Asset to potential cyber attacks without a means to reduce the risk of 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) 7/1/2009 (when the Standard became mandatory and enforceable for Table 1 entities) through 10/26/2009 (Mitigation Plan completion)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY 9/8/2009 and again on 10/20/2009

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-09-2072**
DATE SUBMITTED TO REGIONAL ENTITY **10/20/2009**
DATE ACCEPTED BY REGIONAL ENTITY **10/22/2009**
DATE APPROVED BY NERC **10/27/2009**
DATE PROVIDED TO FERC **10/28/2009**

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

URE submitted an initial Mitigation Plan on September 14, 2009. The Mitigation Plan was rejected by WECC because it indicated that URE was in violation of all sub-requirements of R6. Therefore, WECC requested that URE submit a revised Mitigation Plan documenting R6.5 as the only requirement violated, which URE submitted on October 20, 2009 (as shown above).

MITIGATION PLAN COMPLETED YES NO

EXPECTED COMPLETION DATE **10/30/2009**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **10/26/2009**

DATE OF CERTIFICATION LETTER **10/28/2009 (signed 10/27/2009)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **10/26/2009**

DATE OF VERIFICATION LETTER **12/2/2009**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **10/26/2009**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE modified its CIP-007 R6 Cyber Security procedure to shorten the period of time between log reviews from monthly to weekly to provide a more frequent and consistent manual log analysis process.

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 submitted the following evidence:

- **CIP-007 R6 URE Cyber Security procedure, dated September 24, 2009; and**
- **Manual event log review and the check list forms for weekly review completion.**

EXHIBITS (SEE ATTACHMENTS TO NOTICE OF PENALTY):

SOURCE DOCUMENT
Self-Report dated October 20, 2009

MITIGATION PLAN
Mitigation Plan designated as MIT-09-2072 dated October 20, 2009

CERTIFICATION BY REGISTERED ENTITY
Certification of Mitigation Plan Completion dated October 28, 2009

VERIFICATION BY REGIONAL ENTITY
Verification of Mitigation Plan Completion dated December 2, 2009

Disposition Document for CIP-008-1 R1

DISPOSITION OF VIOLATION
Dated July 12, 2010

NERC TRACKING NO. WECC200901643 REGIONAL ENTITY TRACKING NO. URE_WECC20091816

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRP(S)	VSL(S)
CIP-008-1	1 ¹	1.6	Lower	High

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:

...

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

VIOLATION DESCRIPTION

During a Spot Check conducted by WECC, WECC discovered that URE’s current Cyber Security incident response plan dated 2009 did not include a process for ensuring that the plan is tested at least annually. WECC reviewed a previous Cyber Security incident response plan dated 2008 and confirmed that it included a process for ensuring an annual test. URE expressed that the language addressing annual

¹ CIP-008-1 R1 became mandatory and enforceable for System Control Center Balancing Authorities and Transmission Operators functions on July 1, 2008 and for other facilities’ Balancing Authorities and Transmission Operators functions on July 1, 2009.

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.

testing was inadvertently removed in its 2009 revision of its Cyber Security incident response plan. WECC confirmed that all versions of the plan between and 2009 addressed the process for annual 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 because URE provided evidence to show that its Cyber Security incident response plan had been tested annually even though the annual testing process was not included in the most recent version of the plan.

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) **6/26/2009 (when the annual testing requirement was removed from the plan) through 7/24/2009 (Mitigation Plan completion)**

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

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-09-2374**
DATE SUBMITTED TO REGIONAL ENTITY **7/29/2009 (dated 7/24/2009)**
DATE ACCEPTED BY REGIONAL ENTITY **2/24/2010**
DATE APPROVED BY NERC **3/12/2010**
DATE PROVIDED TO FERC **3/12/2010**

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 **7/24/2009**

DATE OF CERTIFICATION LETTER **7/29/2009 (dated 7/24/2009)**

CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **7/24/2009**

DATE OF VERIFICATION LETTER **3/8/2010**

VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **7/24/2009**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE revised its Cyber Security incident response plan to include a process for ensuring that the plan is reviewed at least annually.

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 submitted its Cyber Security incident response plan V1.5 dated July 22, 2009.

EXHIBITS (SEE ATTACHMENTS TO NOTICE OF PENALTY):

SOURCE DOCUMENT
WECC's Spot Check Screen-shot

MITIGATION PLAN
Mitigation Plan designated as MIT-09-2374 dated July 24, 2009

CERTIFICATION BY REGISTERED ENTITY
Certification of Mitigation Plan Completion dated July 24, 2009

VERIFICATION BY REGIONAL ENTITY
Verification of Mitigation Plan Completion dated March 8, 2010