PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 26, 2011

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

Re: NERC Abbreviated Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP11-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Document (Attachment b), in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This NOP is being filed with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations of CIP-004-1 Requirement (R) 2, R3, and R4, CIP-008-1 R1, and CIP-009-1 R1 and R2. According to the Settlement Agreement, URE neither admits nor denies the violations but stipulates to the facts of the violation and has agreed to the assessed penalty of fifty-nine thousand dollars ($59,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC200901828,

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

[2] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

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

WECC200901829, WECC200901836, WECC201001830, WECC201001831, and WECC201001832 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 October 14, 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-705	WECC200901828	CIP-004-1	2	Medium[3]	7/1/08-5/13/09	59,000
	WECC200901829	CIP-004-1	3	Medium[4]	7/1/08-4/29/09	
	WECC200901836	CIP-004-1	4	Lower[5]	7/1/08-1/15/10	
	WECC201001830	CIP-008-1	1	Lower	7/1/08-6/30/09[6]	
	WECC201001831	CIP-009-1	1	Medium	7/1/08-2/12/10	
	WECC201001832	CIP-009-1	2	Lower	7/1/08-6/24/09	

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

[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. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 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-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[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-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF. When NERC filed VRFs, it originally assigned CIP-004-1 R4.2 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 R4.2 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

[6] The Settlement Agreement states the duration of the CIP-008-1 R1 violation is from July 1, 2008 to June 29, 2008.

CIP-004-1 R2 - OVERVIEW
URE discovered these violations, and self-reported them to WECC. WECC reviewed the Self-Reports at a CIP Spot-Check of URE. WECC determined that URE could not produce evidence demonstrating that personnel were trained within 90 days of being given authorized access to Critical Cyber Assets (CCAs). In addition, URE's training materials prior to May 14, 2009 did not address any of the sub-requirements of CIP-004-1 R2.2.

CIP-004-1 R3 - OVERVIEW
URE discovered these violations, and self-reported them to WECC. WECC reviewed the Self-Reports at a CIP Spot-Check of URE. WECC determined that URE could not produce evidence demonstrating that personnel risk assessments had been performed on certain personnel within 30 days of being granted access to CCAs.

CIP-004-1 R4 - OVERVIEW
URE discovered these violations, and self-reported them to WECC. WECC reviewed the Self-Reports at a CIP Spot-Check of URE. WECC determined that URE could not produce evidence demonstrating that, for certain personnel, URE had updated its access lists and removed access in the time periods allotted by the Standard. In addition, URE access lists used during the audit period did not include specific electronic access rights.

CIP-008-1 R1 - OVERVIEW
This violation was discovered by WECC during the CIP Spot-Check of URE. WECC determined that URE did not have a Cyber Security Incident (CSI) response plan that fully addressed the creation of a process for updating the CSI Plan within 90 calendar days of changes, the creation of a process for ensuring the CSI Plan is reviewed at least annually, or the creation of a process for ensuring the CSI Plan is tested at least annually.

CIP-009-1 R1 - OVERVIEW
This violation was discovered by WECC during the CIP Spot-Check of URE. WECC determined that URE did not have a recovery plan specifically addressing CCAs or the roles and responsibilities of responders.

CIP-009-1 R2 - OVERVIEW
This violation was discovered by WECC during the CIP Spot-Check of URE. WECC determined that URE failed to test its recovery plan at least annually.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[7]

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

[7] *See* 18 C.F.R. § 39.7(d)(4).

Orders,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on April 11, 2011. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a fifty-nine thousand dollar ($59,000) 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. the violations constituted URE's first violation of the subject NERC Reliability Standards;
2. URE self-reported the violations of CIP-004-1 R2,[9] R3, and R4;
3. WECC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which WECC considered a mitigating factor, as discussed in the Disposition Documents;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. 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
7. 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 believes that the assessed penalty of fifty-nine thousand dollars ($59,000) 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 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

[8] *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).

[9] WECC limited self-report credit for CIP-004-1 R2 because the self-report failed to disclose the R2.2 violation.

includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

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

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

Attachments to be included as Part of this Notice of Penalty

The attachments to be included as parts of this NOP are the following documents:

a) Settlement Agreement by and between WECC and URE executed October 14, 2010, included as Attachment 1;
   a) Disposition Document for Common Information, included as Attachment b;
      i. Disposition Document for CIP-004-1 R2, R3, and R4, included as Attachment b.1;
      ii. Disposition Document for CIP-008-1 R1, included as Attachment b.2; and
      iii. Disposition Document for CIP-009-1 R1 and R2, included as Attachment b.3.
   b) Record Documents for CIP-004-1 R2 and R4:
      i. URE's Self-Reporting Form for CIP-004-1 R2, included as Attachment c.1;
      ii. URE's Self-Reporting Form for CIP-004-1 R4, included as Attachment c.2;
      iii. URE's Mitigation Plan MIT-08-3457 for CIP-004-1 R2 and R4, included as Attachment c.3;
      iv. URE's Certification of Mitigation Plan Completion for CIP-004-1 R2 and R4, included as Attachment c.4; and
      v. WECC's Verification of Mitigation Plan Completion for CIP-004-1 R2 and R4, included as Attachment c.5.
   c) Record Documents for CIP-004-1 R3:
      i. URE's Self-Reporting Form for CIP-004-1 R3, included as Attachment d.1;
      ii. URE's Mitigation Plan MIT-08-2364, included as Attachment d.2;
      iii. URE's Certification of Mitigation Plan Completion, included as Attachment d.3; and
      iv. WECC's Verification of Mitigation Plan Completion, included as Attachment d.4.
   d) Record Documents for CIP-008-1 R1:
      i. WECC's Regional Determination of Alleged Violation Summary for CIP-008-1 R1, included as Attachment e.1;
      ii. URE's Mitigation Plan MIT-08-2609, included as Attachment e.2;

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

iii. URE's Certification of Mitigation Plan Completion, included as Attachment e.3; and
iv. WECC's Verification of Mitigation Plan Completion, included as Attachment e.4.

e) Record Documents for CIP-009-1 R1:
i. WECC's Regional Determination of Alleged Violation Summary for CIP-009-1 R1, included as Attachment f.1;
ii. URE's Mitigation Plan MIT-08-2673, included as Attachment f.2;
iii. URE's Certification of Mitigation Plan Completion, included as Attachment f.3; and
iv. WECC's Verification of Mitigation Plan Completion, included as Attachment f.4.

f) Record Documents for CIP-009-1 R2:
i. WECC's Regional Determination of Alleged Violation Summary for CIP-009-1 R2, included as Attachment g.1;
ii. URE's Mitigation Plan MIT-08-2980, included as Attachment g.2;
iii. URE's Certification of Mitigation Plan Completion, included as Attachment g.3; and
iv. WECC's Verification of Mitigation Plan Completion, included as Attachment g.4.

A Form of Notice Suitable for Publication[10]

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

[10] *See* 18 C.F.R. § 39.7(d)(6).

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 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) 883-6855 (801) 883-6894 – facsimile CWhite@wecc.biz Sandy Mooy* Associate General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7658 (801) 883-6894 – facsimile SMooy@wecc.biz	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net Christopher Luras* Manager of Compliance Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

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

Respectfully submitted,

/s/ *Rebecca J. Michael*
Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Sonia C. Mendonça
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

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 b

Disposition Document for Common Information

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment b

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS
Dated April 11, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-705**

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 **$59,000** FOR **SIX** VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

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

LIST VIOLATIONS AND STATUS
ADDITIONAL COMMENTS

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

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

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

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ NO ☐ UNDETERMINED ☐
EXPLAIN
URE has an internal compliance program (ICP) that was in place at the time of the violations and was viewed by WECC as a mitigating factor.

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

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

(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
Reduced Self-Report credit was given applied for CIP-004-1 R2 violation because the Self-Report did not include the full scope of the noncompliance because it did not disclose the R2.2 violation.

OTHER RELEVANT INFORMATION:

NOTICE OF ALLEGED VIOLATION AND PROPOSED PENALTY OR SANCTION ISSUED
DATE: **3/12/10** OR N/A ☐

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **4/30/10** OR N/A ☐

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

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

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

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-1 R2, R3, and R4

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment b.1

DISPOSITION OF VIOLATION
Dated April 1, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901828	**URE_WECC20092068**
WECC200901829	**URE_WECC20092069**
WECC200901836	**URE_WECC20092076**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**2**		**Medium**[1]	**N/A**[2]
CIP-004-1	**3**		**Medium**[3]	**N/A**
CIP-004-1	**4**		**Lower**[4]	**N/A**

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…."

[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. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. The Commission approved the VRF as filed; but, 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 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[2] At the time of the violations, no VSLs were in effect for CIP-004-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[3] 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; but, 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.

[4] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF. When NERC filed VRFs, it originally assigned CIP-004-1 R4.2 a Lower VRF. The Commission approved the VRF as filed; but, 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 R4.2 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

CIP-004-1 R2, R3, and R4 provide:

> **R2. Training — The Responsible Entity[5] 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.**
>
> > **R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.**
> >
> > **R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:**
> >
> > > **R2.2.1. The proper use of Critical Cyber Assets;**
> > >
> > > **R2.2.2. Physical and electronic access controls to Critical Cyber Assets;**
> > >
> > > **R2.2.3. The proper handling of Critical Cyber Asset information; and,**
> > >
> > > **R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.**
> >
> > **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.**
>
> **R3. Personnel Risk Assessment —The Responsible Entity 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 cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that**

[5] 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.

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.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

(Footnote added.)

VIOLATION DESCRIPTION

URE discovered these violations, and self-reported them to WECC. WECC reviewed the Self-Reports at a CIP Spot-Check of URE (Spot-Check). Based on the

findings at the Spot-Check, WECC determined URE had violations of CIP-004-1 R2, R3, and R4.

CIP-004-1 R2:
After reviewing training records with authorized access dates and interviewing URE personnel, the Spot-Check Team found no evidence demonstrating that certain employees, third-party vendor building security personnel, and third-party cleaning personnel with authorized unescorted physical access to URE's control center were given security training within 90 days of being given authorized access to Critical Cyber Assets (CCAs), as required by the Standard. The Spot-Check Team determined that this violation involved fewer than 8% of URE personnel, and those personnel were trained in April of 2009. In addition, after reviewing the training materials presented by URE, the Spot-Check Team determined that URE's training materials used from July 1, 2008 through May 13, 2009 did not address any of the sub-requirements of CIP-004-1 R2.2. The training materials used by URE as of May 14, 2009 addressed all of the requirements of the Standard.

CIP-004-1 R3:
After reviewing documentation provided by URE and interviewing URE personnel, the Spot-Check Team found that URE could not produce evidence demonstrating that certain URE personnel, third-party vendor building security personnel, and third-party cleaning personnel had received personnel risk assessments (PRAs) verifying identification and seven-year criminal checks within 30 days of being granted access to CCAs. The violation involved less than 7% of URE personnel.

CIP-004-1 R4:
After reviewing documentation provided by URE and interviewing URE personnel, the Spot-Check Team found no evidence demonstrating that for certain personnel: (1) URE had updated its access lists as required and (2) had removed access in the time periods allotted by the Standard. In addition, URE access lists used during the audit period did not include specific electronic access rights. Subsequently, URE delivered a newly-created document to the Spot-Check Team that explained the rights that each role granted. This document was not sufficient to demonstrate compliance because (1) it was newly-created and URE did not utilize the document prior to creating it during the Spot-Check, (2) the specific rights were not part of the quarterly review process, so the reviewer would not know what rights had been granted to those on the lists, and (3) the document was informal, and did not have a date, a revision history, or approval information.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

CIP-004-1 R2:
WECC determined that the violations posed a moderate risk to the reliability of the bulk power system (BPS) because there would be a potential impact of inadequately trained personnel not following an entity's expected security practices for CCAs.

The violations did not pose a serious or substantial risk to the BPS because URE did create and implement a training program for which all staff employed by the entity completed. Only third-party contractors, less than 7% of individuals with CCA access did not complete training within specified time period.

CIP-004-1 R3:
WECC determined that the violations posed a moderate risk to the BPS because failing to verify the identity and criminal background of personnel reduces an entity's ability to prevent unintentional or intentional misuse of CCAs. This violation did not pose a serious or substantial risk to the reliability of the BPS because URE did have a PRA program, and implemented this program. The scope of noncompliance was limited to 7% of individuals who did not receive their PRC within 30 days of CCA access. These individuals did complete a PRA which revealed no cause for CCA access-right rejection.

CIP-004-1 R4:
WECC determined that the violations posed a minimal risk to the reliability of the BPS because URE was able to demonstrate with access lists showing timely updating that such revocation lapses are not the norm. While a failure to update access lists can create security risks to an entity's system, this violation did not pose a serious or substantial risk to the reliability of the BPS because URE demonstrated that failure to update is not endemic to its program by providing documentation evidencing timely updates.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT	☒[6]
SELF-CERTIFICATION	☐
COMPLIANCE AUDIT	☐
COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK	☐
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

DURATION DATE(S)

CIP-004-1 R2: 7/1/08 (when URE was required to be compliant with the Standard as a "Table 1 entity") through 5/13/09 (when URE produced training materials addressing all of the Requirements of the Standard)

[6] WECC reduced the Self-Report credit because the Self-Report failed to include the full scope of the violations.

CIP-004-1 R3: 7/1/08 (when URE was required to be compliant with the Standard as a "Table 1 entity") through 4/29/09 (when these personnel received proper PRAs)

CIP-004-1 R4: 7/1/08 (when URE was required to be compliant with the Standard as a "Table 1 entity") through 1/15/10 (Mitigation Plan completion)

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

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

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

III. MITIGATION INFORMATION

CIP-004-1 R3:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-2364**
DATE SUBMITTED TO REGIONAL ENTITY	**12/18/09**
DATE ACCEPTED BY REGIONAL ENTITY	**1/15/10**
DATE APPROVED BY NERC	**3/10/10**
DATE PROVIDED TO FERC	**3/10/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **11/19/09**

DATE OF CERTIFICATION LETTER	**12/22/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**11/19/09**
DATE OF VERIFICATION LETTER	**2/26/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**11/19/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE gave all personnel proper PRAs and put in place updated processes and procedures to ensure PRAs are performed for personnel within 30 days of being given access to CCAs. Corporate PRA duties have been more clearly defined. Company-wide NERC CIP PRAs are documented in the HR NERC CIP database, in the corporate NERC CIP team database, and in the NERC CIP covered units' databases. Online applications notify the section responsible for obtaining the PRA. Checks and balances are built into the process to ensure that those charged with validating PRAs are different from those charged with granting access. The corporate NERC CIP team also makes periodic reviews of the access lists maintained by the Access managers to verify compliance.

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 Personnel Risk Assessment program and PRAs performed by URE's Human Resource Department**

CIP-004-1 R2 and R4:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-3457**[7]
DATE SUBMITTED TO REGIONAL ENTITY	**3/3/10**
DATE ACCEPTED BY REGIONAL ENTITY	**7/6/10**
DATE APPROVED BY NERC	**8/8/10**
DATE PROVIDED TO FERC	**4/4/11**[8]

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

URE submitted a Mitigation Plan to address the self-reported portion of these violations on December 18, 2009, certifying it was completed on November 19, 2009. WECC reviewed this Mitigation Plan and accepted it for the CIP-004-1 R3 violation only, but rejected this Mitigation Plan for the CIP-004-1 R2 and R4 violations because the Mitigation Plan did not address the newly discovered portions of those violations discovered at the Spot-Check. URE revised this Mitigation Plan to

[7] This Mitigation Plan was submitted as a "Revised" Mitigation Plan. Within the Mitigation Plan, references to the CIP-004-1 R3 Mitigation items included in the previously-submitted MIT-08-2364 were removed because the prior Mitigation Plan had been accepted. Therefore, this Mitigation Plan was filed under its own Mitigation Plan Number and not as a "Revised" Mitigation Plan.
[8] Due to an administrative oversight, this Mitigation Plan was not submitted to FERC on time.

include the newly-discovered violations, and submitted the Revised Mitigation Plan on March 3, 2010.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **1/15/10**

DATE OF CERTIFICATION LETTER **3/3/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **1/15/10**

DATE OF VERIFICATION LETTER **7/6/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **1/15/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

CIP-004-1 R2:

URE performed the required training for the personnel involved. URE put in place updated processes and procedures to ensure personnel are given cyber security training within 90 days of being given authorized cyber access or authorized unescorted physical access. Company-wide NERC CIP training responsibilities have been centralized with the corporate NERC CIP team to ensure NERC CIP cyber security training compliance. Company-wide NERC CIP training is documented in the company learning system database, in the corporate NERC CIP team database, and in the NERC CIP covered units' databases. Online applications have been implemented to automate the access requests and training has been given on these automated systems. Checks and balances are built into the process to ensure that those charged with validating training are different from those charged with granting access. The corporate NERC CIP team also makes periodic reviews of the access lists maintained by the Access managers to verify compliance. URE developed an online internal training program that specifically covers the requirements in CIP-004-1 R2.2 (cyber and physical) for CCAs and URE policies related to NERC CIP Standards. All URE employees covered under NERC CIP requirements have taken the current training and provided written acknowledgement of such.

CIP-004-1 R4:

URE added all missing personnel to its access lists. URE has implemented an online application for unescorted physical access to CCAs to automate the Access requests. Once the training and PRA steps are completed, the online application notifies the Facilities Services of that status; the access is provisioned, the access manager is notified and then the official access list is updated. Checks and balances are built into the process to ensure that those

charged with validating training and PRAs are different from those charged with granting access. URE has implemented a new online procedure for cyber access to CAs related the energy management system (EMS). Upon notice of transfer or separation of an individual from HR, System Support personnel checks the current access list. In the event of an individual terminated for cause, System Support personnel are authorized to revoke access for the individual prior to change control approval. In addition, URE put in place updated processes and procedures to ensure that personnel who are given authorized access to CCAs are added to URE's access lists. Finally, URE: (1) updated its access list to depict specific electronic access rights to CCAs, (2) developed a legend detailing the specific access rights for each CCA, and (3) implemented procedures and training to ensure this list is kept current and reviewed in accordance with the CIP requirements.

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)

- **A list that details which individuals have access to which systems, what date the access was provided, what date training was provided, and the date of the last Personnel Risk Assessment**

EXHIBITS:

SOURCE DOCUMENTS
URE's Self-Reporting Form for CIP-004-1 R2

URE's Self-Reporting Form for CIP-004-1 R3
URE's Self-Reporting Form for CIP-004-1 R4

MITIGATION PLAN
URE's Mitigation Plan MIT-08-2364 for CIP-004-1 R3
URE's Revised Mitigation Plan MIT-08-3457for CIP-004-1 R2 and R4

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-004-1 R3

URE's Certification of Mitigation Plan Completion for CIP-004-1 R2 and R4

VERIFICATION BY REGIONAL ENTITY
WECC's Notice of Mitigation Plan and Completed Mitigation Plan Acceptance for CIP-004-1 R3

WECC's Notice of Mitigation Plan and Completed Mitigation Plan Acceptance for CIP-004-1 R2 and R4

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-008-1 R1

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment b.2

DISPOSITION OF VIOLATION
Dated April 11, 2011

NERC TRACKING NO. **WECC201001830**

REGIONAL ENTITY TRACKING NO. **URE_WECC20102070**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-008-1	**1**		**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:

> **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 (ESISAC). The Responsible Entity must ensure that all**

[1] At the time of the violations, no VSLs were in effect for CIP-008-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[2] 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.

reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

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.

(Footnote added.)

VIOLATION DESCRIPTION

This violation was discovered by WECC during the CIP Spot-Check of URE. The Spot-Check Team reviewed all of URE Cyber Security Incident response plan documentation that was in effect during the audit period. The Spot-Check Team determined that during the period of July 1, 2008 through June 29, 2009, URE's Cyber Security Incident response plan (the Plan) documentation did not fully address the creation of a process for updating the Plan within 90 calendar days of changes, the creation of a process for ensuring the Plan is reviewed at least annually, or the creation of a process for ensuring the Plan is tested at least annually. In addition, the documentation provided by URE did not demonstrate that URE had tested its Cyber Security Incident response plan until June 30, 2009.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

The violation posed a minimal risk to the reliability of the bulk power system (BPS). While URE was unable to demonstrate strict compliance with the requirements in CIP-008-1 R1, URE did have portions of a Cyber Incident Response Plan in place that: (1) provided procedures to characterize and classify events as reportable Cyber Security Incidents, (2) addressed response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans; and (3) provided a process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center. In addition, URE had a sabotage reporting procedure that referenced many of the necessary elements required to effectively identify and report a cyber security event.

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 URE was required to be compliant with the Standard as a "Table 1 entity") through 6/30/09 (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- 08-2609**
DATE SUBMITTED TO REGIONAL ENTITY	**3/22/10**
DATE ACCEPTED BY REGIONAL ENTITY	**6/24/10**
DATE APPROVED BY NERC	**7/6/10**
DATE PROVIDED TO FERC	**7/6/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **6/30/09**

DATE OF CERTIFICATION LETTER	**3/22/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**6/30/09**

DATE OF VERIFICATION LETTER **6/25/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **6/30/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE added a documented process in the Cyber Security Incident Response Plan for: (1) updating it within 90 calendar days of any changes, (2) ensuring it is reviewed at least annually, and (3) ensuring it is tested 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's revised Cyber Security Incident Response Plan**

EXHIBITS:

SOURCE DOCUMENT
WECC's Regional Determination of Alleged Violation Summary

MITIGATION PLAN
URE's Mitigation Plan MIT-08-2609

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion

VERIFICATION BY REGIONAL ENTITY
WECC's Notice of Mitigation Plan and Completed Mitigation Plan Acceptance

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-009-1 R1 and R2

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment b.3

DISPOSITION OF VIOLATION
Dated April 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201001831	**URE_WECC20102071**
WECC201001832	**URE_WECC20102072**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-009-1	**1**		**Medium**	**N/A**[1]
CIP-009-1	**2**		**Lower**	**N/A**

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

The purpose statement of CIP-009-1 provides in pertinent part: "Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."

CIP-009-1 R1 and R2 provides:

> **R1. Recovery Plans — The Responsible Entity[2] shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:**
>
> > **R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).**
> >
> > **R1.2. Define the roles and responsibilities of responders.**
>
> **R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper**

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

[2] Within the text of Standard 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.

drill, t o a f ull o perational e xercise, t o r ecovery f rom an actual incident.

(Footnote added.)

VIOLATION DESCRIPTION

These violations were discovered by WECC during the CIP Spot-Check of URE.

CIP-009-1 R1:
The Spot-Check Team reviewed the documentation provided by URE and determined that URE failed to present a recovery plan for CCAs that addressed the recovery of specific CCAs and that addressed events or conditions of varying duration that would activate the recovery plans. In addition, the Spot-Check Team determined that, although URE did have documentation addressing the roles and responsibilities of responders, this documentation was not included in a recovery plan.

CIP-009-1 R2:
The Spot-Check Team reviewed the documentation provided by URE and determined URE failed to present evidence demonstrating it had tested its recovery plan at least annually. Specifically, the time gap between the first exercise of the recovery plan in 2008, and the second exercise of the recovery plan was held 14 months and 23 days later.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

CIP-009-1 R1:
The violation posed a moderate risk to the reliability of the bulk power system (BPS) because failing to have a recovery plan meeting all qualifications of the Standard could cause a significant delay to the recovery of CCAs. Although URE's recovery plan for R1 did not include documented procedures for recovery of each CCA individually, URE had in place both hardware and software tools and procedures to respond broadly to disasters, failures and emergencies. Specifically, URE was using tape backup hardware and software to backup CCAs, and had in place documented vendor procedures to recover CCAs in the event of failure. In addition, URE also has a maintenance contract in place with its EMS vendor for emergencies and has hardware maintenance contracts in place for hardware emergencies. These techniques and practices defined the roles and responsibilities of the vendor responders. In fact, URE did experience a hard disk failure on one of URE's CCAs during the period at issue. Support personnel were able to utilize the procedures in place at URE to successfully ensure the continued safe and reliable operation of the URE system. URE rebuilt procedures for 39 of its 43 identified CCAs. Based on the existence of these rebuilt procedures, URE would most likely have been able to recover CCAs following an event involving the unavailability of

CCAs. In addition, while URE did not address the roles and responsibilities of responders in the recovery plan, those roles and responsibilities were included in other URE documents.

CIP-009-1 R2:
The violation posed a minimal and not serious or substantial risk to the reliability of the BPS because a delay of two months and 24 days is not likely to have a significant impact on reliability. The recovery plan was ultimately tested after this short delay.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

CIP-009-1 R1:
DURATION DATE(S) **7/1/08 (when URE was required to be compliant with the Standard as a "Table 1 entity") through 2/12/10 (Mitigation Plan completion)**

CIP-009-1 R2:
DURATION DATE(S) **7/1/08 (when URE was required to be compliant with the Standard as a "Table 1 entity") through when the recovery plan was tested**

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

CIP-009-1 R1:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-2673**
DATE SUBMITTED TO REGIONAL ENTITY	**3/22/10**
DATE ACCEPTED BY REGIONAL ENTITY	**7/9/10**
DATE APPROVED BY NERC	**8/12/10**
DATE PROVIDED TO FERC	**8/12/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **2/12/10**

DATE OF CERTIFICATION LETTER	**3/22/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**2/12/10**
DATE OF VERIFICATION LETTER	**7/19/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**2/12/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE created an individual Recovery Plan for CCAs that is separate and apart from URE's recovery plan for the system as a whole.

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 Recovery Plan for Critical Cyber Assets**

CIP-009-1 R2:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-2980**
DATE SUBMITTED TO REGIONAL ENTITY	**3/22/10**
DATE ACCEPTED BY REGIONAL ENTITY	**7/6/10**
DATE APPROVED BY NERC	**8/8/10**
DATE PROVIDED TO FERC	**11/17/10**[3]

[3] Due to an administrative oversight, this Mitigation Plan was not submitted to FERC on time.

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **6/24/09**

DATE OF CERTIFICATION LETTER **3/22/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **6/24/09**

DATE OF VERIFICATION LETTER **7/7/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **6/24/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE tested its Recovery Plan. The Recovery Plan was subsequently re-tested eight months later in 2010, after URE completed its revised Recovery Plan for CCAs.

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)

- **WECC reviewed the Annual Test of CCA Recovery Plan 2010 and 2011. WECC also reviewed CCA Recovery Plan Exercise 2010. WECC SME interviewed entity on 7/6/2010.**

EXHIBITS:

SOURCE DOCUMENT
WECC's Regional Determination of Alleged Violation Summary for CIP-009-1 R1

WECC's Regional Determination of Alleged Violation Summary for CIP-009-1 R2

MITIGATION PLAN
URE's Mitigation Plan MIT-08-2673 for CIP-009-1 R1

URE's Mitigation Plan MIT-08-2980 for CIP-009-1 R2

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment b.3

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-009-1 R1

URE's Certification of Mitigation Plan Completion for CIP-009-1 R2

VERIFICATION BY REGIONAL ENTITY
WECC's Notice of Mitigation Plan and Completed Mitigation Plan Acceptance for CIP-009-1 R1

WECC's Notice of Mitigation Plan and Completed Mitigation Plan Acceptance for CIP-009-1 R2