PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

April 29, 2011

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

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

Dear Ms. Bose:

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

This NOP is being filed with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the enforceable violations of CIP-004-1 Requirement (R) 4, CIP-005-1 R4, CIP-007-1 R1, CIP-007-1 R2, CIP-007-1 R3, CIP-007-1 R4, CIP-007-1 R5, CIP-007-1 R6, CIP-007-1 R7, CIP-007-1 R8, CIP-008-1 R1, CIP-009-1 R2 and CIP-009-1 R5. According to the Settlement Agreement, URE stipulates to the facts of the violation, and has agreed to the assessed penalty of eighty nine thousand dollars ($89,000), in

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

[2] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2010). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

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

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 WECC200901729, WECC200901730, WECC200901731, WECC200901732, WECC200901733, WECC200901734, WECC200901735, WECC200901736, WECC200901737, WECC200901738, WECC200901855,[3] WECC200901851 and WECC200901864 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 August 6, 2010, by and between WECC and URE. The details of the findings and the basis for the penalty are set forth in the Disposition Documents. This NOP filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7, NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
NOC-649	WECC200901729	CIP-004-1	4	Lower	7/1/09-9/28/09	89,000
	WECC200901730	CIP-005-1	4	Medium	7/1/09-12/14/09	
	WECC200901731	CIP-007-1	1	Medium	7/1/09-12/3/09	
	WECC200901732	CIP-007-1	2	Medium	7/1/09-12/3/09	
	WECC200901733	CIP-007-1	3	Lower	7/1/09-12/3/09	
	WECC200901734	CIP-007-1	4	Medium	7/1/09-12/3/09	
	WECC200901735	CIP-007-1	5	Lower	7/1/09-9/29/09	
	WECC200901736	CIP-007-1	6	Medium	7/1/09-3/19/10	
	WECC200901737	CIP-007-1	7	Lower	7/1/09-9/28/09	
	WECC200901738	CIP-007-1	8	Medium	7/1/09-12/30/09	
	WECC200901855	CIP-008-1	1	Lower	7/1/09-9/28/09	
	WECC200901851	CIP-009-1	2	Lower	7/1/09-9/18/09	
	WECC200901864	CIP-009-1	5	Lower	7/1/09-10/27/09	

[3] The Settlement Agreement incorrectly identifies the NERC Violation ID as WECC201001855.

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

Within the text of Standard CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

CIP-004-1 R4- OVERVIEW
URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 24, 2009. WECC determined that URE failed to maintain lists of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs), including their specific electronic and physical access rights to CCAs.

CIP-005-1 R4- OVERVIEW
URE discovered this violation on September 8, 2009 and self-reported it to WECC on September 18, 2009. WECC determined that URE failed to perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter (ESP) at least annually.

CIP-007-1 R1- OVERVIEW
URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 24, 2009. WECC determined that URE failed to create, implement and maintain cyber security test procedures ensuring that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls as required by the Standard.

CIP-007-1 R2- OVERVIEW
URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 24, 2009. WECC determined that URE failed to establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

CIP-007-1 R3- OVERVIEW
URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 24, 2009. WECC determined that URE did not establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP.

CIP-007-1 R4- OVERVIEW
URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 30, 2009. WECC determined that URE did not use anti-virus software and other malicious software (malware) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the ESP.

CIP-007-1 R5- OVERVIEW

URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 30, 2009. WECC determined that URE did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

CIP-007-1 R6- OVERVIEW

URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 24, 2009. WECC determined that URE did not ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

CIP-007-1 R7- OVERVIEW

URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 24, 2009. WECC determined that URE did not establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the ESP as identified and documented in Standard CIP-005.

CIP-007-1 R8- OVERVIEW

URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 24, 2009. WECC determined that URE did not perform a cyber vulnerability assessment of all Cyber Assets within the ESP at least annually.

CIP-008-1 R1- OVERVIEW

URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 24, 2009. WECC determined that URE did not have a Cyber Security Incident response plan which included procedures to characterize and classify events as reportable Cyber Security Incidents, response actions, reporting incidents, response plan annual review and a process for testing the plan.

CIP-009-1 R2- OVERVIEW

URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 24, 2009. WECC determined that URE did not exercise its recovery plan(s) for CCAs as required by the Standard.

CIP-009-1 R5- OVERVIEW

URE discovered this violation on June 12, 2009 and self-reported it to WECC on June 24, 2009. WECC determined that URE had not tested information essential to recovery that is stored on backup media as of July 1, 2009 when URE was required to be compliant with the Standard.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

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,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on January 10, 2011. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of an eighty nine thousand dollar ($89,000) 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 occurrence of violation of the subject NERC Reliability Standards;
2. URE self-reported the violations;
3. WECC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violations 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;
7. URE's had implemented compliance procedures which led to the discover of these violations, which WECC considered a mitigating factor, 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 approves the Settlement Agreement and believes that the assessed penalty of eighty nine thousand dollars ($89,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *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).

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30 day period following the filing of this NOP with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

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

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

Attachments to be included as Part of this Notice of Penalty

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

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

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

   i. Disposition Document for CIP-004-1 R4, included as Attachment b-1;

   ii. Disposition Document for CIP-005-1 R4, included as Attachment b-2;

   iii. Disposition Document for CIP-007-1 R1, R2, R3, R4, R5, R6, R7 and R8, included as Attachment b-3;

   iv. Disposition Document for CIP-008-1 R1, included as Attachment b-4; and

   v. Disposition Document for CIP-009-1 R2 and R5, included as Attachment b-5.

c) Record Documents for CIP-004-1 R4:

   i. URE's Self-Report for CIP-004-1 R4 dated June 24, 2009, included as Attachment c-1;

   ii. URE's Mitigation Plan MIT-09-2153 submitted June 24, 2009, included as Attachment c-2;

   iii. URE's Certification of Mitigation Plan Completion dated September 29, 2009, included as Attachment c-3; and

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

iv. WECC's Verification of Mitigation Plan Completion dated December 2, 2009, included as Attachment c-4.

d) Record Documents for CIP-005-1 R4:

i. URE's Self-Report for CIP-005-1 R4 dated September 18, 2009, included as Attachment d-1;

ii. URE's Mitigation Plan MIT-09-2154 submitted September 18, 2009, included as Attachment d-2;

iii. URE's Certification of Mitigation Plan Completion dated December 15, 2009, included as Attachment d-3; and

iv. WECC's Verification of Mitigation Plan Completion dated January 11, 2010, included as Attachment d-4.

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

i. URE's Self-Report for CIP-007-1 R1 dated June 24, 2009, included as Attachment e-1;

ii. URE's Revised Mitigation Plan MIT-09-2155 dated November 19, 2009 and submitted November 20, 2009, included as Attachment e-2;

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

iv. WECC's Verification of Mitigation Plan Completion dated September 15, 2010, included as Attachment e-4.

f) Record Documents for CIP-007-1 R2:

i. URE's Self-Report for CIP-007-1 R2 dated June 24, 2009, included as Attachment f-1;

ii. URE's Mitigation Plan MIT-09-2196 submitted June 24, 2009, included as Attachment f-2;

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

iv. WECC's Verification of Mitigation Plan Completion dated March 24, 2010, included as Attachment f-4.

g) Record Documents for CIP-007-1 R3:

i. URE's Self-Report for CIP-007-1 R3 dated June 24, 2009, included as Attachment g-1;

ii. URE's Mitigation Plan MIT-09-2176 submitted June 24, 2009, included as Attachment g-2;

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

iv. WECC's Verification of Mitigation Plan Completion dated March 24, 2010, *see* Attachment f-4.

h) Record Documents for CIP-007-1 R4:

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

i. URE's Self-Report for CIP-007-1 R4 dated June 30, 2009, included as Attachment h-1;

ii. URE's Revised Mitigation Plan MIT-09-2177 dated November 19, 2009 and submitted November 20, 2009, included as Attachment h-2;

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

iv. WECC's Verification of Mitigation Plan Completion dated March 25, 2010, included as Attachment h-4.

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

i. URE's Self-Report for CIP-007-1 R5 dated June 30, 2009, included as Attachment i-1;

ii. URE's Mitigation Plan MIT-09-2156 submitted June 30, 2009, included as Attachment i-2;[6]

iii. URE's Certification of Mitigation Plan Completion dated September 29, 2009, included as Attachment i-3; and

iv. WECC's Verification of Mitigation Plan Completion dated December 2, 2009, included as Attachment i-4.

j) Record Documents for CIP-007-1 R6:

i. URE's Self-Report for CIP-007-1 R6 dated June 24, 2009, included as Attachment j-1;

ii. URE's Revised Mitigation Plan MIT-09-2234 submitted November 25, 2009, included as Attachment j-2;

iii. URE's Revised Mitigation Plan MIT-09-2234 submitted January 27, 2010, included as Attachment j-3;

iv. URE's Certification of Mitigation Plan Completion dated March 22, 2010, included as Attachment j-4; and

v. WECC's Verification of Mitigation Plan Completion dated September 10, 2010, included as Attachment j-5.

k) Record Documents for CIP-007-1 R7:

i. URE's Self-Report for CIP-007-1 R7 dated June 24, 2009, included as Attachment k-1;

ii. URE's Mitigation Plan MIT-09-2178 submitted June 24, 2009, included as Attachment k-2;

iii. URE's Certification of Mitigation Plan Completion dated September 29, 2009, included as Attachment k-3; and

[6] The Settlement Agreement at page 13 incorrectly states the Mitigation Plan was submitted to WECC on June 24, 2009.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

iv. WECC's Verification of Mitigation Plan Completion dated December 18, 2009, included as Attachment k-4.

l) Record Documents for CIP-007-1 R8:

i. URE's Self-Report for CIP-007-1 R8 dated June 24, 2009, included as Attachment l-1;

ii. URE's Mitigation Plan MIT-09-2157 submitted June 24, 2009, included as Attachment l-2;

iii. URE's Certification of Mitigation Plan Completion signed December 31, 2009, included as Attachment l-3; and

iv. WECC's Verification of Mitigation Plan Completion dated September 20, 2010, included as Attachment l-4.

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

i. URE's Self-Report for CIP-008-1 R1 dated June 24, 2009, included as Attachment m-1;

ii. URE's Mitigation Plan MIT-09-2421 submitted June 24, 2009, included as Attachment m-2;

iii. URE's Certification of Mitigation Plan Completion dated September 29, 2009, included as Attachment m-3; and

iv. WECC's Verification of Mitigation Plan Completion dated April 1, 2010, included as Attachment m-4.

n) Record Documents for CIP-009-1 R2:

i. URE's Self-Report for CIP-009-1 R2 dated June 24, 2009, included as Attachment n-1;

ii. URE's Revised Mitigation Plan MIT-09-2409 submitted August 26, 2009, included as Attachment n-2;

iii. URE's Certification of Mitigation Plan Completion dated September 29, 2009, included as Attachment n-3; and

iv. WECC's Verification of Mitigation Plan Completion dated June 7, 2010, included as Attachment n-4.

o) Record Documents for CIP-009-1 R5:

i. URE's Self-Report for CIP-009-1 R5 dated June 24, 2009, included as Attachment o-1;

ii. URE's Revised Mitigation Plan MIT-09-2416 submitted September 18, 2009, included as Attachment o-2;

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

iv. WECC's Verification of Mitigation Plan Completion dated June 7, 2010, included as Attachment o-4.

A Form of Notice Suitable for Publication[7]

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

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* Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, N.J. 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) 883-6885 (801) 883-6894 – facsimile CWhite@wecc.biz Sandy Mooy* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7658 (801) 883-6894 – facsimile SMooy@wecc.biz	Rebecca J. Michael* Assistant General Counsel Davis Smith* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, D.C. 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net davis.smith@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.

[7] *See* 18 C.F.R. § 39.7(d)(6).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

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

Respectfully submitted,

/s/ *Rebecca J. Michael*

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Sr. Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
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

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 January 10, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXX**	**NOC-649**

REGIONAL ENTITY
Western Electricity Coordinating Council (WECC)

IS THERE A SETTLEMENT AGREEMENT YES ☒ NO ☐

WITH RESPECT TO THE VIOLATION(S), REGISTERED ENTITY

NEITHER ADMITS NOR DENIES IT (SETTLEMENT ONLY) YES ☐
ADMITS TO IT YES ☒
Stipulates to the facts
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 **$89,000** FOR **THIRTEEN** 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.

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

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

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ NO ☐ UNDETERMINED ☐
EXPLAIN
WECC evaluated URE's Internal Compliance Program and found it to be a mitigating factor in determining the penalty amount.

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

OTHER RELEVANT INFORMATION:

NOTICE OF ALLEGED VIOLATION AND PROPOSED PENALTY OR SANCTION ISSUED
DATE: **1/4/10** OR N/A ☐
SETTLEMENT DISCUSSIONS COMMENCED
DATE: **2/5/10 for WECC200901729 through WECC200901738 and 5/14/10 for WECC200901855,[2] WECC200901851 and WECC2009018647** 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

[2] The Settlement Agreement incorrectly refers to this violation tracking number as WECC201001855.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-1 R4

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

DISPOSITION OF VIOLATION
Dated January 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901729	**URE_WECC20091907**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**4**	**4.1**	**Lower**[1]	**N/A**[2]

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

The purpose statement of CIP-004-1 provides in pertinent part: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."

CIP-004-1 R4 provides:

> **Access — The Responsible Entity[3] 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.**

[1] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF.
[2] At the time of the violation, no VSLs were in effect for CIP-004-1. On June 30, 2009, NERC submitted VSLs for the CIP-002 through CIP-009 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.
[3] Within the text of Standard CIP-004, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

> **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

In a Self-Report dated June 24, 2009, URE indicated that it did not have a process for maintaining a list of personnel with authorized access to Critical Cyber Assets (CCAs), including their specific electronic and physical access privileges. URE discovered the violation through its compliance process.[4] URE also indicated that it did not have a process for ensuring review of the list quarterly or updating the list within seven calendar days of any change of personnel or access rights. Also, URE did not have a process for revoking access in accordance with CIP-004-1 R4.

WECC Enforcement reviewed URE's Self-Report and the findings of the WECC subject matter experts (SMEs) and determined that URE has a violation of this Reliability Standard requirement because URE failed to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs.

On February 3, 2010, URE responded to the Notice of Alleged Violation and Proposed Penalty or Sanction (NAVAPS) and contested this violation stating that while it did not have a procedure for maintaining lists which was the basis for its Self-Report, it did maintain lists of personnel with authorized cyber or authorized unescorted physical access since prior to its compliant date of July 1, 2009. URE further stated that it has reviewed and updated these lists and revoked access as needed. Subsequently, WECC SMEs reviewed evidence presented by URE to demonstrate compliance with this Standard. WECC SMEs determined that the documentation presented by URE was sufficient to demonstrate compliance with this Standard with the exception of one instance where one employee retired and the access list was not updated within seven days as required by the Standard.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that this violation did not pose a serious or substantial risk to the bulk power system (BPS). URE violation was limited to a single employee. Specifically, URE s failed to update the access within seven days pursuant to R4.1. Further, the entity's implementation of physical and cyber access controls, which require physical access to the CCA in order to operate the device, mitigated the risk

[4] For background information leading to the discovery of these violations, *See* Attachment b: Disposition Document for Common Information § II (6).

of unauthorized cyber or physical access to CCAs. Also, the entity's small employee base leads to an entity culture in which employees are familiar with those having access to CCAs. Thus, it is unlikely that unauthorized physical CCA access would occur.

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 URE was subject to compliance with the Standard) through 9/28/09 (Mitigation Plan completion)**[5]

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **6/24/09**

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2153**
DATE SUBMITTED TO REGIONAL ENTITY	**6/24/09 (signed 6/23/09)**
DATE ACCEPTED BY REGIONAL ENTITY	**11/12/09**
DATE APPROVED BY NERC	**12/2/09**
DATE PROVIDED TO FERC	**12/2/09**

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

[5] The Settlement Agreement incorrectly states that the violation duration is from August 8, 2009 until September 8, 2009.

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **9/30/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **9/28/09**

DATE OF CERTIFICATION LETTER **9/29/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **9/28/09**

DATE OF VERIFICATION LETTER **12/2/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **9/28/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE formalized its procedure for maintaining a list of personnel with authorized or authorized unescorted physical access to CCAs and the corresponding electronic and physical access rights. The procedure includes quarterly reviews and updates that are within the requirements of CIP-004 R4 (seven calendar days of any change or within 24 hours for personnel terminated for cause).

URE developed, documented, and approved a process to maintain lists of personnel with authorized access to CCAs and/or physical access rights to CCAs. The list includes each person's access rights and privileges, the authorizing entity and date/time authorized. In addition the list is secured such that only authorized personnel can review it and only relevantly authorized personnel can add, delete or modify its contents.

URE developed and documented a mechanism for ensuring the list(s) of personnel who have access to CCAs are updated within a maximum of seven calendar days of any change in the access rights of any personnel, including permanent staff, contractors and vendors.

URE developed and documented a mechanism to ensure that access to CCAs is revoked within seven working days for a person who no longer requires such access including employees/contractors/vendors that cease to be employed by the client. This process is accelerated to within 24 hours for any employee/contractor/vendor whose employment is terminated with cause.

URE purchased the "OATI webCompliance" program and implemented the program for document management, automatic alerts and reminders associated with CIP-004-1 R4.

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)

- **Access procedure**
- **list of internal access rights, permissions to Critical Cyber Assets to the PSP and ESP**
- **list of vendor access rights to Critical Cyber Assets**
- **List of employees requiring background checks pursuant to NERC CIP mandatory standard**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-004-1 R4 dated June 24, 2009

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2153 submitted June 24, 2009

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion dated September 29, 2009

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-005-1 R4

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

DISPOSITION OF VIOLATION
Dated January 10, 2011

NERC TRACKING NO. **WECC200901730**

REGIONAL ENTITY TRACKING NO. **URE_WECC20091909**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-005-1	**4**		**Medium**	**N/A**[1]

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

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

CIP-005-1 R4 provides:

> **Cyber Vulnerability Assessment — The Responsible Entity[2] shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:**
>
> > **R4.1. A document identifying the vulnerability assessment process;**
> >
> > **R4.2. A review to verify that only ports and services required for operations at these access points are enabled;**
> >
> > **R4.3. The discovery of all access points to the Electronic Security Perimeter;**
> >
> > **R4.4. A review of controls for default accounts, passwords, and network management community strings; and,**

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

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

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

(Footnote added.)

VIOLATION DESCRIPTION

In a Self-Report dated September 18, 2009, URE indicated that it had failed to perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) (ESP) at least annually. URE discovered the violation through its compliance process.[3] URE stated that it was non-compliant because, although URE has a document identifying the vulnerability process to perform an assessment of cyber vulnerability of electronic access points within the ESP, URE did not understand that it must perform an annual assessment by the compliant date of July 1, 2009 and therefore had not performed the annual assessment as required. Therefore, URE does not have documentation of its annual assessment as required by CIP-005-1 R4.2 through R4.5.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that this violation did not pose a serious or substantial risk to the bulk power system (BPS) because URE has an isolated physical network which links only to the Balancing Authority via a secured, firewalled ICCP link. In addition, although URE could not establish that it had performed an annual assessment by its compliant date, URE did have procedures to perform the assessment annually. Although URE is a relatively small entity which has somewhat limited ability to impact the BPS, WECC determined that this violation posed a moderate risk to the reliability of the BPS.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

[3] For background information leading to the discovery of these violations, *See* Attachment b: Disposition Document for Common Information § II (6).

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

DURATION DATE(S) **7/1/09 (when URE was required to be compliant with the Standard) through 12/14/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **9/18/09**

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2154**
DATE SUBMITTED TO REGIONAL ENTITY	**9/18/09**
DATE ACCEPTED BY REGIONAL ENTITY	**11/12/09**
DATE APPROVED BY NERC	**12/2/09**
DATE PROVIDED TO FERC	**12/2/09**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**12/15/09**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**12/14/09**

DATE OF CERTIFICATION LETTER	**12/15/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**12/14/09**

DATE OF VERIFICATION LETTER	**1/11/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**12/14/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE completed a cyber vulnerability assessment of the electronic access points to the ESP. The assessment included a review to verify that only those ports and services required for operations of access points are enabled; discovery of access points, and a review of controls for default accounts, passwords, and network management community strings.

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)

- **Procedure for conducting the assessment of the Cyber vulnerability**
- **Results of the assessment of the Cyber vulnerability**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-005-1 R4 dated September 18, 2009

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2154 submitted September 18, 2009

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion dated December 15, 2009

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion dated January 11, 2010

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007-1 R1, R2, R3, R4, R5, R6, R7 and R8

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

DISPOSITION OF VIOLATION
Dated January 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901731	**URE_WECC20091910**
WECC200901732	**URE_WECC20091911**
WECC200901733	**URE_WECC20091912**
WECC200901734	**URE_WECC20091913**
WECC200901735	**URE_WECC20091914**
WECC200901736	**URE_WECC20091915**
WECC200901737	**URE_WECC20091916**
WECC200901738	**URE_WECC20091917**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	**1**		**Medium**	**N/A**[1]
CIP-007-1	**2**		**Medium**	**N/A**
CIP-007-1	**3**		**Lower**	**N/A**
CIP-007-1	**4**		**Medium**	**N/A**
CIP-007-1	**5**		**Lower**	**N/A**
CIP-007-1	**6**		**Medium**	**N/A**
CIP-007-1	**7**		**Lower**	**N/A**
CIP-007-1	**8**		**Medium**	**N/A**

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

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

[1] At the time of the violations, no VSLs were in effect for CIP-007-1. On June 30, 2009, NERC submitted VSLs for the CIP-002 through CIP-009 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-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.

CIP-007-1 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.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

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

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

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

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

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.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

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

R7. Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

(Footnotes added.)

CIP-007-1 R1 VIOLATION DESCRIPTION

In a Self-Report dated June 24, 2009, URE indicated that it failed to create, implement, and maintain cyber security test procedures for new Cyber Assets or significant changes to existing Cyber Assets within the Electronic Security Perimeter (ESP) in a manner that minimized adverse effects on the production system or its operation. URE discovered the violation through its compliance process.[3]

CIP-007-1 R1 RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the violation did not pose a serious or substantial risk to the bulk power system (BPS) because the risk is mitigated by URE's isolation of its ESP and its policy of not implementing significant change within the ESP until adequate test procedures are in place for such changes. WECC SMEs determined URE did not assess or implement processes to ensure that Cyber Asset changes within the ESP did not adversely affect cyber security. The absence of a test procedure for new Cyber Assets or significant changes to existing Cyber Assets has not impacted cyber operations or reliability. Although URE is a relatively small entity which has

[3] For background information leading to the discovery of all these violations, See Attachment b: Disposition Document for Common Information§ II (6).

somewhat limited ability to impact the BPS, WECC determined that this violation posed a moderate risk to the reliability of the BPS.

CIP-007-1 R2 VIOLATION DESCRIPTION

URE discovered the violation through its compliance process. In a Self-Report dated June 24, 2009, URE indicated that a process to ensure that only those ports and services required for normal and emergency operations are enabled did not exist at URE as required by CIP-007-1 R2. URE indicated that it did not have a process to verify that only those ports and services required for normal and emergency operations are enabled and all other ports and services are disabled.

CIP-007-1 R2 RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC found the impact of the violation on the BPS was moderate and not serious or substantial because URE has an isolated physical network which links only to the Balancing Authority via a secured, firewalled ICCP link. The absence of a procedure to manage ports and services has not impacted cyber operations or reliability due the isolated nature of the network. Although URE is a relatively small entity which has somewhat limited ability to impact the BPS, WECC determined that this violation posed a moderate risk to the reliability of the BPS.

CIP-007-1 R3 VIOLATION DESCRIPTION

URE discovered the violation through its compliance process. In a Self-Report dated June 24, 2009, URE indicated that a procedure for security patch management did not exist at URE. WECC Enforcement reviewed URE's Self-Report and the findings of the WECC SMEs and determined that URE had a violation of this Standard because URE did not establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP.

CIP-007-1 R3 RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC found that this violation did not pose a serious or substantial risk to the BPS because URE has an isolated physical network which links only to the Balancing Authority via a secured, firewalled ICCP link. The absence of a security patch management procedure has not impacted cyber operations or reliability due the isolated nature of the network, which reduces the need for security patches. This Standard does not pose a significant risk to the BPS if an entity is complying with the ESP requirements, as such, WECC SMEs determined that URE was complying with the ESP requirements, and therefore CIP-007-1 R3 posed a minimal risk to the reliability of the BPS.

CIP-007-1 R4 VIOLATION DESCRIPTION

URE discovered the violation through its compliance process. In a Self-Report dated June 30, 2009, URE indicated that a procedure for malicious software prevention did not exist at URE in accordance with CIP-007-1 R4. WECC SMEs determined that URE could not demonstrate that it had deployed anti-virus and other malicious software prevention tools where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within its ESP.

CIP-007-1 R4 RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined the impact to the BPS was not serious or substantial because URE has an isolated physical network which links only to the Balancing Authority via a secured, firewalled ICCP link. The absence of a malicious software prevention procedure has not impacted cyber operations or reliability due to the isolated nature of the network. Although URE is a relatively small entity which has somewhat limited ability to impact the BPS, WECC determined that this violation posed a moderate risk to the reliability of the BPS.

CIP-007-1 R5 VIOLATION DESCRIPTION

URE discovered the violation through its compliance process. In a Self-Report dated June 30, 2009, URE indicated that a process for account management did not exist at URE in accordance with CIP-007-1 R5. URE did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access as required by CIP-007-1 R5.

CIP-007-1 R5 RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that this violation did not pose a serious or substantial risk to the BPS because URE took precautions to minimize risk of unauthorized system access even in the absence of an account management procedure. While URE did not have a documented process for account management, URE maintained shared accounts only when necessary. Where possible, URE disabled generic and factory default accounts. User accounts were required for individual logins to Cyber Assets. Authorized access permission were consistent with the concept of "need to know" with respect to work functions performed. Access logs were created such that an audit trail of user account access activity was available. Passwords were set at a minimum of seven characters and require a combination of alpha, numeric, and special characters. URE practiced adequate account management, but had not documented its practices. For these reasons, WECC determined that this violation posed a minimal risk to the BPS.

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

CIP-007-1 R6 VIOLATION DESCRIPTION

URE discovered the violation through its compliance process. In a Self-Report dated June 24, 2009, URE indicated that it was in violation of CIP-007-1 R6 because URE failed to document and implement a procedure for security status monitoring in accordance with this Standard. WECC Enforcement reviewed the Self-Report and the findings of the WECC SMEs and found that URE did not have a procedure in place to ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

CIP-007-1 R6 RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that this violation did not have a serious or substantial impact on the BPS because URE has an isolated physical network. The absence of a security status monitoring procedure has not impacted cyber operations or reliability due the isolated nature of the network. Although URE is a relatively small entity which has somewhat limited ability to impact the BPS, WECC determined that this violation posed a moderate risk to the reliability of the BPS.

CIP-007-1 R7 VIOLATION DESCRIPTION

URE discovered the violation through its compliance process. In a Self-Report dated June 24, 2009, URE indicated that it did not establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the ESP as identified and documented in Standard CIP-005. WECC Enforcement reviewed the URE's Self-Report and the findings of the WECC SMEs and determined that URE did not have a process for ensuring any potentially sensitive data contained on media used within the ESP is destroyed before disposal or redeployment of assets or otherwise prevent unauthorized retrieval of sensitive cyber security or reliability data related to disposal or redeployment of Cyber Assets.

CIP-007-1 R7 RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that this violation did not pose a serious or substantial risk to the BPS because URE had not disposed of or redeployed any identified Cyber Assets within the ESP. Any obsolete or out of service Cyber Assets are securely stored within the Physical Security Perimeter (PSP). For these reasons, WECC determined that this violation posed a minimal risk to the BPS.

CIP-007-1 R8 VIOLATION DESCRIPTION

URE discovered the violation through its compliance process. In a Self-Report dated June 24, 2009, URE indicated that it did not have a procedure in place to

perform a cyber vulnerability assessment of Cyber Assets within the ESP at least annually. WECC SMEs determined that URE failed to perform and document an annual vulnerability assessment of Cyber Assets within the ESP. URE did not understand that it must perform a "bookend" annual assessment prior to the compliant date of July 1, 2009 and therefore had not performed the annual assessment as required.

CIP-007-1 R8 RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that this violation did not pose a substantial or serious risk to the BPS because URE has an isolated physical network. The absence of a cyber vulnerability assessment procedure has not impacted operations or reliability due the isolated nature of the network, which minimizes the vulnerability of Cyber Assets. Although URE is a relatively small entity which has somewhat limited ability to impact the BPS, WECC determined that this violation posed a moderate risk to the reliability of the BPS.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) **R1: 7/1/09 (when URE was required to be compliant with the Standard) through 12/3/09 (Mitigation Plan completion)**

R2: 7/1/09 (when URE was required to be compliant with the Standard) through 12/3/09 (Mitigation Plan completion)

R3: 7/1/09 (when URE was required to be compliant with the Standard) through 12/3/09 (Mitigation Plan completion)

R4: 7/1/09 (when URE was required to be compliant with the Standard) through 12/3/09 (Mitigation Plan completion)
R5: 7/1/09 (when URE was required to be compliant with the Standard) through 9/29/09 (Mitigation Plan completion)

R6: 7/1/09 (when URE was required to be compliant with the Standard) through 3/19/10 (Mitigation Plan completion)

R7: 7/1/09 (when URE was required to be compliant with the Standard) through 9/28/09 (Mitigation Plan completion)

R8: 7/1/09 (when URE was required to be compliant with the Standard) through 12/30/09 (Mitigation Plan completion)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **6/24/09 (R1, R2, R3, R6, R7 and R8) and 6/30/09 (R4 and R5)**

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-007-1 R1:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2155**
DATE SUBMITTED TO REGIONAL ENTITY	**11/20/09**[4]
DATE ACCEPTED BY REGIONAL ENTITY	**11/20/09**
DATE APPROVED BY NERC	**12/2/09**
DATE PROVIDED TO FERC	**12/2/09**

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

URE submitted a Mitigation Plan to address this violation on June 24, 2009 with an expected completion date of September 30, 2009. On November 12, 2009, WECC SMEs reviewed and accepted this Mitigation Plan. On September 29, 2009, URE certified completion of this Mitigation Plan. On November 12, 2009, WECC SMEs reviewed URE's cyber security test procedures and determined that they were not adequate for compliance with the Standard and that URE had not completed the Mitigation Plan because URE's cyber security test procedures only address the functionality aspect of significant changes to Cyber Assets, and did not address the cyber security effects of significant changes on the Cyber Assets.

MITIGATION PLAN COMPLETED YES ☒ NO ☐
EXPECTED COMPLETION DATE **12/4/09**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **12/3/09**

[4] The Mitigation Plan is dated November 19, 2009.

DATE OF CERTIFICATION LETTER	**12/4/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**12/3/09**
DATE OF VERIFICATION LETTER	**9/15/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**12/3/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE formalized its test procedures to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls. The procedure is inclusive to the requirements of CIP-007-1 R1, which consists of test procedure to minimize the effects on the production system, documentation that testing is performed, and documentation of the test results. URE revised the process to include security testing for new Cyber Assets or significant changes to existing Cyber Assets.

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)

Cyber Security test procedures
Template for the Cyber Security test control procedure

CIP-007-1 R2:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2196**
DATE SUBMITTED TO REGIONAL ENTITY	**6/24/09**
DATE ACCEPTED BY REGIONAL ENTITY	**12/10/09**
DATE APPROVED BY NERC	**12/28/09**
DATE PROVIDED TO FERC	**12/28/09**

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

EXPECTED COMPLETION DATE	**9/30/09**
EXTENSIONS GRANTED	**12/4/09**[5]
ACTUAL COMPLETION DATE	**12/3/09**

[5] The original approved completion date was September 30, 2009 and URE certified completion of this Mitigation Plan on September 29, 2009, certifying that it was completed that same day. WECC informed URE on November 18, 2009 that WECC had not accepted the completion of the Mitigation Plan. URE submitted its next Certification document on December 4, 2009.

DATE OF CERTIFICATION LETTER **12/4/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **12/3/09**

DATE OF VERIFICATION LETTER **3/24/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **12/3/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE formalized a process to ensure only ports and services required for normal and emergency operations are enabled. URE developed, documented, approved, and implemented a procedure to address ports and services in accordance with CIP-007-1 R2. The process defines required ports and services and ensures that only those ports and services required for normal and emergency operations are enabled.

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)
Procedure to address ports and services

CIP-007-1 R3:
FOR FINAL ACCEPTED MITIGATION PLAN:
MITIGATION PLAN NO. **MIT-09-2176**
DATE SUBMITTED TO REGIONAL ENTITY **6/24/09**
DATE ACCEPTED BY REGIONAL ENTITY **12/10/09**
DATE APPROVED BY NERC **12/18/09**
DATE PROVIDED TO FERC **12/18/09**
IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **9/30/09**
EXTENSIONS GRANTED **12/4/09**[6]
ACTUAL COMPLETION DATE **12/3/09**

DATE OF CERTIFICATION LETTER **12/4/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **12/3/09**

[6] The original approved completion date was September 30, 2009 and URE certified completion of this Mitigation Plan on September 29, 2009, certifying that it was completed that same day. WECC informed URE on November 18, 2009 that WECC had not accepted the completion of the Mitigation Plan. URE submitted the next Certification document on December 4, 2009.

DATE OF VERIFICATION LETTER	**3/24/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**12/3/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE formalized a process for security patch management including: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP. According to the process, URE will document the assessment of security patches and upgrades within thirty calendar days of availability and document implementation of security patches. In the case a patch is not installed, compensating measures will be applied to mitigate risk exposure or an acceptance of risk.

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)

Process for security patch management
Test procedures for the security patch management process

CIP-007-1 R4:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2177**
DATE SUBMITTED TO REGIONAL ENTITY	**11/20/09**[7]
DATE ACCEPTED BY REGIONAL ENTITY	**12/10/09**
DATE APPROVED BY NERC	**12/18/09**
DATE PROVIDED TO FERC	**12/18/09**

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

URE submitted a Mitigation Plan to address this violation on June 24, 2009 with an expected completion date of September 30, 2009. On November 12, 2009, WECC SMEs reviewed and accepted this Mitigation Plan. On September 29, 2009, URE certified completion of this Mitigation Plan. On November 12, 2009, WECC SMEs reviewed URE's cyber security test procedures and determined that they were not adequate for compliance with the Standard and that URE had not completed the Mitigation Plan because URE's cyber security test procedures only address the functionality aspect of significant changes to Cyber Assets, and did not address the cyber security effects of significant changes on the Cyber Assets.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

[7] The Mitigation Plan is dated November 19, 2009.

EXPECTED COMPLETION DATE **9/30/09**
EXTENSIONS GRANTED **11/18/09**[8]
ACTUAL COMPLETION DATE **12/3/09**

DATE OF CERTIFICATION LETTER **12/4/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **12/3/09**

DATE OF VERIFICATION LETTER **3/25/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **12/3/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE is now using anti-virus software to detect, prevent, deter and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the ESP. URE has formalized a process for updating the anti-virus software and malware prevention "signatures." The process addresses testing and installing the signatures.

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)

Process for updating anti-virus software and malicious software protection

CIP-007-1 R5:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **MIT-09-2156**
DATE SUBMITTED TO REGIONAL ENTITY **6/30/09**[9]
DATE ACCEPTED BY REGIONAL ENTITY **11/20/09**
DATE APPROVED BY NERC **12/2/09**
DATE PROVIDED TO FERC **12/2/09**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

[8] The original approved completion date was September 30, 2009 and URE certified completion of this Mitigation Plan on September 29, 2009, certifying that it was completed that same day. WECC informed URE on November 18, 2009 that WECC had not accepted the completion of the Mitigation Plan. URE submitted the next Certification document on December 4, 2009.
[9] The Settlement Agreement states the Mitigation Plan was submitted on June 24, 2009.

EXPECTED COMPLETION DATE **9/30/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **9/29/09**

DATE OF CERTIFICATION LETTER **9/29/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **9/29/09**

DATE OF VERIFICATION LETTER **12/2/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **9/29/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE has formalized a process for account management. URE designed, documented and implemented a control process to enforce access authentication and accountability for all user activity, such that unauthorized activity is minimized or eliminated.

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)
Process for account management

CIP-007-1 R6:
FOR FINAL ACCEPTED MITIGATION PLAN:
MITIGATION PLAN NO. **MIT-09-2234**
DATE SUBMITTED TO REGIONAL ENTITY **1/27/10**
DATE ACCEPTED BY REGIONAL ENTITY **5/28/10**
DATE APPROVED BY NERC **6/29/10**
DATE PROVIDED TO FERC **6/29/10**

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

URE submitted a Mitigation Plan to address this violation on June 24, 2009 with an expected completion date of September 30, 2009. URE certified completion of this Mitigation Plan on September 30, 2009, certifying that it was completed on September 28, 2009.

After discussions with WECC SMEs, URE submitted a revised Mitigation Plan on November 25, 2009 that was accepted by WECC on December 9, 2009, approved by NERC on January 5, 2010 and sent to FERC on January 5, 2010. After submitting the revised Mitigation Plan, URE hired a consultant to help evaluate the processes and tools to meet strict compliance. The scheduled implementation of this solution

was February 9, 2010 through February 10, 2010 and so URE requested an extension of the completion date to March 31, 2010 in the final Mitigation Plan submitted January 27, 2010.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **2/25/10**
EXTENSIONS GRANTED **3/31/10**[10]
ACTUAL COMPLETION DATE **3/19/10**

DATE OF CERTIFICATION LETTER **3/22/10 (submitted 3/23/10)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **3/19/10**

DATE OF VERIFICATION LETTER **9/10/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **3/19/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE has taken a number of steps to meet compliance of CIP-007 R6. URE has hired a consultant, and with the help of the consultant, URE evaluated a number of tools available on the market to accomplish automated security status monitoring. URE purchased the highest evaluated solution of both hardware and software that accomplishes the goal of providing robust security status monitoring of Cyber Assets, and installed this solution February 9, 2010 through February 10, 2010.

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED, LIST EVIDENCE REVIEWED FOR COMPLETED MILESTONES)
Procedure for Security status monitoring and screen shots demonstrating its new procedure.

CIP-007-1 R7:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **MIT-09-2178**
DATE SUBMITTED TO REGIONAL ENTITY **6/24/09**
DATE ACCEPTED BY REGIONAL ENTITY **12/9/09**
DATE APPROVED BY NERC **12/18/09**
DATE PROVIDED TO FERC **12/18/09**

[10] On January 5, 2010, NERC sent FERC an approved Mitigation Plan for CIP-007-1 R6 as designated by WECC. WECC subsequently provided a revised Mitigation Plan in which URE added the additional steps of (1) adding documentation updates to its procedures and (2) training on the procedures and tools. The additional steps changed the approved completion date from February 25, 2010 to March 31, 2010.

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **9/30/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **9/28/09**

DATE OF CERTIFICATION LETTER **9/29/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **9/28/09**

DATE OF VERIFICATION LETTER **12/18/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **9/28/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE developed, documented, approved, and implemented a procedure to address disposal and redeployment of Cyber Assets in accordance with CIP-007-1 R7. URE designed and documented a process for ensuring any potentially sensitive data contained on media used within the ESP is destroyed before disposal or redeployment of assets. Finally, URE maintains records that such assets were disposed of or redeployed in accordance with documented procedures.

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)

- **Procedure to address disposal and redeployment of Cyber Assets**
- **Process for ensuring any potentially sensitive data contained on media used within the ESP is destroyed before disposal or redeployment of assets.**
- **Sample of a record that shows an asset that was disposed of or redeployed in accordance with documented procedures.**

CIP-007-1 R8:
OR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **MIT-09-2157**
DATE SUBMITTED TO REGIONAL ENTITY **6/24/09**
DATE ACCEPTED BY REGIONAL ENTITY **11/12/09**
DATE APPROVED BY NERC **12/2/09**
DATE PROVIDED TO FERC **12/2/09**

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **12/31/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **12/30/09**

DATE OF CERTIFICATION LETTER **12/31/09**[11]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **12/30/09**

DATE OF VERIFICATION LETTER **9/20/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **12/30/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE enlisted an SME to perform a cyber vulnerability assessment. Specifically, the SME developed, produced, and documented a method of reliable annual assessment of cyber vulnerability inclusive of the requirements of the Standard. URE ensured that the assessment process includes a review of ports and services and a review of controls and default accounts. The cyber vulnerability assessment will also include full documentation of the results of the assessment. If vulnerabilities are identified, action plans will be proposed to remediate or mitigate vulnerabilities identified in the assessment, and URE will do a post-assessment following the mitigation of vulnerabilities to ensure that mitigation as been completed and documented. Finally, URE will obtain the necessary budgetary approval and document minimum expectations of the resource.

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)
Procedure for cyber vulnerability assessment
Results from the cyber vulnerability assessment

[11] The Certification of Completion incorrectly states it was submitted on June 24, 2009.

CIP-007-1 R1 EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R1 dated June 24, 2009

MITIGATION PLAN
URE's Revised Mitigation Plan MIT-09-2155 dated November 19, 2009 and submitted November 20, 2009

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

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion dated September 15, 2010

CIP-007-1 R2 EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R2 dated June 24, 2009

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2196 submitted June 24, 2009

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

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion dated March 24, 2010

CIP-007-1 R3 EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R3 dated June 24, 2009

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2176 submitted June 24, 2009

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

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion dated March 24, 2010

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

CIP-007-1 R4 EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R4 dated June 30, 2009

MITIGATION PLAN
URE's Revised Mitigation Plan MIT-09-2177 dated November 19, 2009 and submitted November 20, 2009

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

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion dated March 25, 2010

CIP-007-1 R5 EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R5 dated June 30, 2009

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2156 submitted June 30, 2009

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion dated September 29, 2009

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

CIP-007-1 R6 EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R6 dated June 24, 2009

MITIGATION PLAN
URE's Revised Mitigation Plan MIT-09-2234 submitted November 25, 2009
URE's Revised Mitigation Plan MIT-09-2234 submitted January 27, 2010

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion dated March 22, 2010

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion dated September 10, 2010

CIP-007-1 R7 EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R7 dated June 24, 2009

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2178 submitted June 24, 2009

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion dated September 29, 2009

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion dated December 18, 2009

CIP-007-1 R8 EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R8 dated June 24, 2009

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2157 submitted June 24, 2009

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion signed December 31, 2009

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion dated September 20, 2010

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-4

DISPOSITION OF VIOLATION
Dated January 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901855[1]	**URE_WECC20092104**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-008-1	**1**		**Lower**	**N/A**[2]

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:

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

[1] The Settlement Agreement incorrectly states the NERC Violation ID as WECC201001855.
[2] At the time of the violation, no VSLs were in effect for CIP-007-1. On June 30, 2009, NERC submitted VSLs for the CIP-002 through CIP-009 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.
[3] 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.

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

In a Self-Report dated June 24, 2009, URE indicated that it did not have a Cyber Security Incident response plan including procedures to characterize and classify events as reportable Cyber Security Incidents, response actions, reporting incidents, response plan annual review and a process for testing the plan as required by the Standard. URE discovered the violation through its compliance process.[4] On March 15, 2010, WECC subject matter experts (SME) reviewed URE's Self-Report. Based on this Self-Report and discussions with URE personnel, WECC SMEs determined that URE did not have a Cyber Security Incident response plan addressing the requirements of the Standard. WECC Enforcement reviewed the Self-Report and the SME's findings and determined that URE had a violation of CIP-008-1 R1 because it did not have a Cyber Security Incident response plan addressing the requirements of the Standard.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC found that the violation did not pose a serious or substantial risk to the bulk power system (BPS) because URE has an isolated physical network. Due to the isolated nature of the network, the possibility of a URE incurring a Cyber Security Incident is minimal as would be the affect on operations or reliability. In addition, URE had been identifying Critical Assets and Critical Cyber Assets (CCAs) and was monitoring these assets for Cyber Security Incidents reportable under CIP-008-1 R1.1 and R2.

[4] For background information leading to the discovery of these violations, *See* Attachment b: Disposition Document for Common Information§ II (6).

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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 URE was required to be compliant with the Standard) through 9/28/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **6/24/09**

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2421**
DATE SUBMITTED TO REGIONAL ENTITY	**6/24/09 (signed 6/23/09)**
DATE ACCEPTED BY REGIONAL ENTITY	**3/22/10**
DATE APPROVED BY NERC	**3/30/10**
DATE PROVIDED TO FERC	**3/30/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**9/30/09**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**9/28/09**

DATE OF CERTIFICATION LETTER	**9/29/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**9/28/09**

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

DATE OF VERIFICATION LETTER **4/1/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **9/28/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE formalized its Cyber Security Incident response plan. The plan characterizations and classifications of events along with response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans. A method for reporting Cyber Security Incidents to the ES ISAC is included in the plan. The plan will be updated within 90 calendar days of any changes and reviewed 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)

- **Cyber Security Incident response plan**
- **Model for the Cyber Incident reporting form for ES ISAC**
- **URE Cyber Incident reporting form**
- **URE's Procedure for the Cyber drill**
- **Cyber Security Incident drill template**
- **Results of the Cyber Security Incident drill**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-008-1 R1 dated June 24, 2009

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2421 submitted June 24, 2009

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion dated September 29, 2009

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion dated April 1, 2010

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-009-1 R2 and R5

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment b-5

DISPOSITION OF VIOLATION
Dated January 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901851	**URE_WECC20092092**
WECC200901864	**URE_WECC20092114**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-009-1	**2**		**Lower**	**N/A**[1]
CIP-009-1	**5**		**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[2] 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 R2 provides: "Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident."

CIP-009-1 R5 provides: "Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site."

VIOLATION DESCRIPTION

CIP-009-1 R2:

In a Self-Report dated June 24, 2009, URE indicated that it had not exercised its recovery plan(s) for Critical Cyber Assets (CCAs) as of July 1, 2009 when URE was

[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 through CIP-009 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.

required to be compliant with the Standard. URE discovered the violation through its compliance process.[3] URE did not understand that it must perform an initial exercise by the compliant date of July 1, 2009 and therefore had not performed the annual exercise as required.

CIP-009-1 R5:

In a Self-Report dated June 24, 2009, URE indicated that it did not have a procedure for annually testing backup media. WECC SMEs determined that URE had not tested information essential to recovery that is stored on backup media as of July 1, 2009 when URE was required to be compliant with the Standard. URE did not understand that it must perform an initial test by the compliant date of July 1, 2009 and therefore had not performed the test as required.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

CIP-009-1 R2:

WECC determined that the risk to the reliability of the bulk power system (BPS) was not serious or substantial because even though failure to exercise recovery plans for CCAs increases the potential risk that recovery plans are inadequate and that CCAs are out of service for longer than necessary, URE is a relatively small entity with a somewhat limited ability to impact the BPS. In addition, URE had been identifying Critical Assets and CCAs, and had developed a recovery plan for CCAs that would have been used in the event recovery was needed. URE has not had any events or conditions in the past that would require implementation of a recovery plan.

CIP-009-1 R5:

WECC found that this violation did not pose a serious or substantial risk to the BPS because URE uses software to automatically run backups of its Cyber Assets at the primary control center and backup control center. URE regularly checks the status and reports from its software to ensure that backups are running as scheduled and no errors are reported. While URE checks the status of backups and backup logs, URE has not documented the procedure or tested its backup media. URE has not had any incidents in the past requiring recovery from a backup.

[3] For background information leading to the discovery of these violations, See Attachment b: Disposition of Violation § II (6).

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) **R2: 7/1/09 (when URE was required to be compliant with the Standard) through 9/18/09 (date of the recovery plan paper drill)**

R5: 7/1/09 (when URE was required to be compliant with the Standard) through 10/27/09 (Mitigation Plan completion)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **6/24/09**

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

III. MITIGATION INFORMATION

CIP-009-1 R2:

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2409**
DATE SUBMITTED TO REGIONAL ENTITY	**8/26/09**
DATE ACCEPTED BY REGIONAL ENTITY	**3/9/10**
DATE APPROVED BY NERC	**3/24/10**
DATE PROVIDED TO FERC	**3/24/10**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE
URE submitted a Mitigation Plan to address this violation on June 24, 2009 which was accepted by WECC, URE submitted a revised Mitigation Plan on August 26, 2009 to modify the timeline.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **9/30/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **9/29/09**

DATE OF CERTIFICATION LETTER **9/29/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **9/29/09**

DATE OF VERIFICATION LETTER **6/7/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **9/29/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE developed, documented, and approved procedure for annually exercising the recovery plan for CCAs. URE has purchased the "OATI webCompliance" program and implemented the program for document management, and automatic alerts and reminders associated with CIP-009-1 R2. URE completed a paper drill of the recovery plan. Although the exercise was a paper drill, the backup media was checked to validate the information on the media tape was available for recovery.

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)

- **CCA Recovery Plans**
- **URE Recovery Plan Exercise**

CIP-009-1 R5:

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **MIT-09-2416**
DATE SUBMITTED TO REGIONAL ENTITY **6/30/09**
DATE ACCEPTED BY REGIONAL ENTITY **3/16/10**
DATE APPROVED BY NERC **3/25/10**
DATE PROVIDED TO FERC **3/25/10**

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

URE submitted subsequent revisions to the Mitigation Plan to update milestone dates on August 26, 2009 and September 23, 2009.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **10/31/09**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **10/27/09**

DATE OF CERTIFICATION LETTER **10/28/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **10/27/09**

DATE OF VERIFICATION LETTER **6/7/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **10/27/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE developed, documented, approved and implemented a procedure for annually testing backup media. Once the procedure was completed, URE implemented the procedure and executed a backup media test in accordance with the Standard. In addition, URE purchased an "OATI webCompliance" program for document management and automatic alerts and reminders associated with CIP-009-1 R5.

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)

- **CCA Recovery Plans**
- **URE's backup media test of the primary control center and the backup control center**

CIP-009-1 R2 EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-009-1 R2 dated June 24, 2009

MITIGATION PLAN
URE's Revised Mitigation Plan MIT-09-2409 submitted August 26, 2009

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion dated September 29, 2009

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion dated June 7, 2010

CIP-009-1 R5 EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report dated June 24, 2009

MITIGATION PLAN
URE's Revised Mitigation Plan MIT-09-2416 submitted September 18, 2009

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

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion dated June 7, 2010