PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 28, 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). This NOP includes 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 violations of CIP-002-1 Requirement (R) 1 and R3, CIP-003-1 R1, R2, and R3, CIP-007-1 R1, and CIP-009-1 R1. According to the Settlement Agreement, URE agrees to the stipulated facts of the violations and has agreed to the assessed penalty of seventy-five thousand dollars ($75,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201001843, WECC201001844,

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

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

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

WECC201001845, WECC201001846, WECC201001847, WECC200901818, and WECC201001874 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 December 21, 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-751	WECC201001843	CIP-002-1	1	Medium[3]	7/1/08-12/3/10	75,000
	WECC201001844	CIP-002-1	3	High[4]	7/1/08-5/14/10	
	WECC201001845	CIP-003-1	1	Medium[5]	7/1/08-8/10/10	

[3] When NERC filed Violation Risk Factors (VRF) it originally assigned CIP-002-1 R1 and R1.2 Lower VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on January 27, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-002-1 R1 and R1.2 were in effect from June 18, 2007 until January 27, 2009 when the Medium VRFs became effective. CIP-002-1 R1 and R1.2 are each assigned a Medium VRF and CIP-002-1 R1.1, R1.2.1, R1.2.2, R1.2.3, R1.2.4, R1.2.5, R1.2.6 and R1.2.7 are each assigned a Lower VRF. WECC originally assigned this violation a Lower VRF during its initial review and then determined that the Medium VRF was the appropriate VRF.

[4] When NERC filed VRFs it originally assigned CIP-002-1 R3 a Medium VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on January 27, 2009, the Commission approved the modified High VRF. Therefore, the Medium VRF for CIP-002-1 R3 was in effect from June 18, 2007 until January 27, 2009 when the High VRF became effective. CIP-002-1 R3 is assigned a High VRF and CIP-002-1 R3.1, R3.2 and R3.3 are each assigned a Lower VRF. WECC originally assigned this violation a Medium VRF during its initial review and then determined that the High VRF was the appropriate VRF.

[5] CIP-003-1 R1 has a Medium VRF; R1.1, R1.2 and R1.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-003-1 R1 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the Medium VRF became effective. WECC originally assigned this violation a Lower VRF during its initial review and then determined that the Medium VRF was the appropriate VRF.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

	WECC201001846	CIP-003-1	2	Medium[6]	8/26/08-12/16/09	
	WECC201001847	CIP-003-1	3	Lower	7/1/08-6/19/09	
	WECC200901818	CIP-007-1	1	Medium[7]	7/1/08-5/14/09	
	WECC201001874	CIP-009-1	1	Medium	1/1/10-1/9/10	

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

CIP-002-1 R1 - OVERVIEW
This violation was discovered during a WECC Spot Check[8] of URE. WECC determined that URE had a Risk-Based Assessment Methodology (RBAM) which failed to (1) document procedures and evaluation criteria and their application to systems and facilities critical to system restoration (R1.2.4) and (2) document its consideration of Special Protection Systems (R1.2.6).

CIP-002-1 R3 - OVERVIEW
This violation was discovered during a WECC Spot Check of URE. WECC determined that URE failed to classify energy management system (EMS) operator consoles, critical to the operation of the EMS and, therefore, essential to the operation of a Critical Asset, as Critical Cyber Assets.

CIP-003-1 R1 - OVERVIEW
This violation was discovered during a WECC Spot Check of URE. WECC determined that URE failed to document 30 requirements in Reliability Standards CIP-002 through CIP-009 in its cyber security policy.

CIP-003-1 R2 - OVERVIEW
This violation was discovered during a WECC Spot Check of URE. WECC determined that URE failed to identify its designated senior manager's title, business phone, and business address in its cyber security policy during the period between August 26, 2008 and December 15, 2009.

[6] CIP-003-1 R2 has a Medium VRF; R2.1, R2.2 and R2.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-003-1 R2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-003-1 R2 was in effect from June 18, 2007 until January 27, 2009, when the Medium VRF became effective. WECC originally assigned this violation a Lower VRF during its initial review and then determined that the Medium VRF was the appropriate VRF.

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

[8] The Settlement Agreement uses the term "Spot Check Audit," this was a Spot Check of URE and not an audit.

CIP-003-1 R3 - OVERVIEW
This violation was discovered during a WECC Spot Check of URE. WECC determined that URE had five documented exceptions covering 15 instances related to account and password management on URE's EMS consoles which required exceptions and therefore failed to document exceptions to its cyber security policy within 30 days of those exceptions being approved by the Senior Manager.

CIP-007-1 R1 - OVERVIEW
URE discovered the violation of CIP-007-1 R1 during a self-evaluation, and self-reported the violation. WECC determined that URE had procedures in place to consider the impact on existing cyber security controls of adding or modifying Critical Cyber Assets within the Electronic Security Perimeter, but such procedures did not consider the impact of adding or modifying non-critical Cyber Assets.

CIP-009-1 R1 - OVERVIEW
URE reported violation of CIP-009-1 R1 through both the Self-Report and Self-Certification processes. WECC determined that URE did not have a recovery plan for one of its generating stations, a Critical Cyber Asset, until January 9, 2010.

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

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines, the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[10] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on July 11, 2011. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a seventy-five thousand dollar ($75,000) 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:[11]

1. the violations constituted URE's first violation of the subject NERC Reliability Standards;
2. URE self-reported the violation of CIP-007-1 R1;
3. WECC reported that URE was cooperative throughout the compliance enforcement process;

[9] *See* 18 C.F.R. § 39.7(d)(4).
[10] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).
[11] URE did not receive credit for having a compliance program because it was not reviewed by WECC.

4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), as discussed in the Disposition Documents; and
6. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of seventy-five thousand dollars ($75,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

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

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

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

Attachments to be included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between WECC and URE executed December 16, 2010, included as Attachment 1;
   a) Disposition Document for Common Information, included as Attachment b;
      i. Disposition Document for CIP-002-1 R1 and R3, included as Attachment b.1;
      ii. Disposition Document for CIP-003-1 R1, R2, and R3, included as Attachment b.2;
      iii. Disposition Document for CIP-007-1 R1included as Attachment b.3; and

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

iv. Disposition Document for CIP-009-1 R1, included as Attachment b.4.

b) Record Documents for CIP-002-1 R1:
   i. WECC's Regional Determination of Alleged Violation Summary for CIP-002-1 R1, included as Attachment c.1;
   ii. URE's Mitigation Plan MIT- 08-3669, included as Attachment c.2;
   iii. URE's Certification of Mitigation Plan Completion, included as Attachment c.3; and
   iv. WECC's Verification of Mitigation Plan Completion, included as Attachment c.4.
c) Record Documents for CIP-002-1 R3:
   i. WECC's Regional Determination of Alleged Violation Summary for CIP-002-1 R3, included as Attachment d.1;
   ii. URE's Mitigation Plan MIT-08-2796, included as Attachment d.2;
   iii. URE's Certification of Mitigation Plan Completion, included as Attachment d.3; and
   iv. WECC's Verification of Mitigation Plan Completion, included as Attachment d.4.
d) Record Documents for CIP-003-1 R1:
   i. WECC's Regional Determination of Alleged Violation Summary for CIP-003-1 R1, included as Attachment e.1;
   ii. URE's Mitigation Plan MIT-08-2534, included as Attachment e.2;
   iii. URE's Certification of Mitigation Plan Completion, included as Attachment e.3; and
   iv. WECC's Verification of Mitigation Plan Completion, included as Attachment e.4.
e) Record Documents for CIP-003-1 R2:
   i. WECC's Regional Determination of Alleged Violation Summary for CIP-003-1 R2, included as Attachment f.1;
   ii. URE's Mitigation Plan MIT-08-2725, included as Attachment f.2;
   iii. URE's Certification of Mitigation Plan Completion, included as Attachment f.3; and
   iv. WECC's Verification of Mitigation Plan Completion, included as Attachment f.4.
f) Record Documents for CIP-003-1 R3:
   i. WECC's Regional Determination of Alleged Violation Summary for CIP-003-1 R3, included as Attachment g.1;
   ii. URE's Mitigation Plan MIT-08-2726, included as Attachment g.2;
   iii. URE's Certification of Mitigation Plan Completion, included as Attachment g.3; and
   iv. WECC's Verification of Mitigation Plan Completion, included as Attachment g.4.
g) Record Documents for CIP-007-1 R1:
   i. URE's Compliance Violation Self-Reporting Form for CIP-007-1 R1, included as Attachment h.1;
   ii. URE's Mitigation Plan MIT-08-2735, included as Attachment h.2;

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

iii. URE's Certification of Mitigation Plan Completion, included as Attachment h.3; and

iv. WECC's Verification of Mitigation Plan Completion, included as Attachment h.4.

h) Record Documents for CIP-009-1 R1:

i. URE's Self-Certification for CIP-009-1 R1, included as Attachment i.1;

ii. URE's Mitigation Plan MIT-10-2832, included as Attachment i.2;

iii. URE's Certification of Mitigation Plan Completion, included as Attachment i.3; and

iv. WECC's Verification of Mitigation Plan Completion, included as Attachment i.4.

A Form of Notice Suitable for Publication[12]

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

[12] *See* 18 C.F.R. § 39.7(d)(6).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 213-2673 (801) 582-3918 – facsimile Mark@wecc.biz Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6855 (801) 883-6894 – facsimile CWhite@wecc.biz Sandy Mooy* Associate General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7658 (801) 883-6894 – facsimile SMooy@wecc.biz	Rebecca J. Michael* Associate General Counsel for Regulatory and Corporate Matters Sonia C. Mendonca* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net Christopher Luras* Manager of Compliance Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

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

Respectfully submitted,

/s/ *Rebecca J. Michael*

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

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 July 11, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-751**

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 **$75,000** FOR **SEVEN** VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

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

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☐ NO ☐ UNDETERMINED ☒
EXPLAIN
URE did not receive credit for having a compliance program because it was not reviewed by WECC.

EXPLAIN SENIOR MANAGEMENT'S ROLE AND INVOLVEMENT WITH RESPECT TO THE REGISTERED ENTITY'S COMPLIANCE PROGRAM, INCLUDING WHETHER SENIOR MANAGEMENT TAKES ACTIONS THAT SUPPORT THE COMPLIANCE PROGRAM, SUCH AS TRAINING, COMPLIANCE AS A FACTOR IN EMPLOYEE EVALUATIONS, OR OTHERWISE.

(4) ANY ATTEMPT BY THE REGISTERED ENTITY TO CONCEAL THE VIOLATION(S) OR INFORMATION NEEDED TO REVIEW, EVALUATE OR INVESTIGATE THE VIOLATION.

YES ☐ NO ☒
IF YES, EXPLAIN

(5) ANY EVIDENCE THE VIOLATION(S) WERE INTENTIONAL (IF THE RESPONSE IS "YES," THE ABBREVIATED NOP FORM MAY NOT BE USED.)

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

NOTICE OF ALLEGED VIOLATION AND PROPOSED PENALTY OR SANCTION ISSUED
DATE: **4/14/10** OR N/A ☐

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **5/14/10** OR N/A ☐

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

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

REGISTERED ENTITY RESPONSE CONTESTED
FINDINGS ☐ PENALTY ☐ BOTH ☐ DID NOT CONTEST ☒
HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-002-1 R1 and R3

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERION

Attachment b.1

DISPOSITION OF VIOLATION

Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201001843	**URE_WECC20102084**
WECC201001844	**URE_WECC20102085**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-002-1[1]	**1**	**1.2.4, 1.2.6**	**Medium**[2]	**N/A**[3]
CIP-002-1	**3**		**High**[4]	**N/A**

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

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

[1] CIP-002-1 was in effect from July 1, 2008 until April 1, 2010 when CIP-002-2 became effective. CIP-002-2 was in effect t from April 1, 2010 until October 1, 2010 when CIP-002-3 became effective. The violations span multiple versions of this Standard, but the subsequent versions do not change the meaning of the original NERC Reliability Standard and its requirements. For consistency in this filing, the original Standard CIP-002-1 is used throughout.

[2] When NERC filed Violation Risk Factors (VRF) it originally assigned CIP-002-1 R1 and R1.2 Lower VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on January 27, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-002-1 R1 and R1.2 were in effect from June 18, 2007 until January 27, 2009 when the Medium VRFs became effective. CIP-002-1 R1 and R1.2 are each assigned a Medium VRF and CIP-002-1 R1.1, R1.2.1, R1.2.2, R1.2.3, R1.2.4, R1.2.5, R1.2.6 and R1.2.7 are each assigned a Lower VRF. WECC originally assigned this violation a Lower VRF during its initial review and then determined that the Medium VRF was the appropriate VRF.

[3] At the time of the violations, no Violation Severity Levels (VSLs) were in effect for CIP-002-1. 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.

[4] When NERC filed VRFs it originally assigned CIP-002-1 R3 a Medium VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on January 27, 2009, the Commission approved the modified High VRF. Therefore, the Medium VRF for CIP-002-1 R3 was in effect from June 18, 2007 until January 27, 2009 when the High VRF became effective. CIP-002-1 R3 is assigned a High VRF and CIP-002-1 R3.1, R3.2 and R3.3 are each assigned a Lower VRF. WECC originally assigned this violation a Medium VRF during its initial review and then determined that the High VRF was the appropriate VRF.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERION

CIP-002-1R1 and R3 provide:

> **R1. Critical Asset Identification Method — The Responsible Entity[5] shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.**
>
> > **R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.**
> >
> > **R1.2. The risk-based assessment shall consider the following assets:**
> >
> > > **R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.**
> > >
> > > **R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.**
> > >
> > > **R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.**
> > >
> > > **R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.**
> > >
> > > **R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.**
> > >
> > > **R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.**
> > >
> > > **R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.**

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

> **R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:**
>
> > **R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,**
> >
> > **R3.2. The Cyber Asset uses a routable protocol within a control center; or,**
> >
> > **R3.3. The Cyber Asset is dial-up accessible.**

(Footnote added.)

VIOLATION DESCRIPTION

CIP-002-1 R1:
This violation was discovered during a WECC Spot Check of URE (Spot Check). The Spot Check team established that URE did not have blackstart generation capabilities, and was dependent on outside entities in blackstart situations. URE's Risk-Based Assessment Methodology (RBAM) failed to address a possible loss of transmission lines in the electrical path of blackstart facilities. As a result, URE's RBAM failed to include two of five substations critical to system restoration on its 2009 Critical Assets List. One of the URE facilities not identified as a Critical Asset was required for initial system restoration in six of eight URE blackout restoration procedures reviewed by WECC.

URE's RBAM also failed to include a risk-based assessment methodology for Special Protection Systems. The URE RBAM also lacked sufficient detail in its evaluation criteria to generate reliable assessment results. URE did not document its decision to remove four substations from its Critical Asset List during URE's 2009 application of its RBAM sufficiently.

WECC Enforcement reviewed the Spot Check findings and determined that URE had a violation of CIP-002-1 R2 because it failed to (1) document procedures and evaluation criteria and their application to systems and facilities critical to system

restoration (R1.2.4) and (2) document its consideration of Special Protection Systems (R1.2.6).

CIP-002-1 R3:
The Spot Check team and WECC Enforcement determined that URE failed to identify its operator consoles as Critical Cyber Assets essential to the operation of a Cyber Asset on its Critical Assets List. The Critical Cyber Asset serves as the human machine interface , essential to the operation power operations of Critical Assets.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

CIP-002-1 R1:
The violation posed a moderate risk to the reliability of the bulk power system (BPS) because the failure to apply specific consideration for critical facilities may affect reliable operation. The violation was not a serious or substantial risk to the BPS because URE did adopt and implement an RBAM and did annually apply its RBAM to create URE's list of Critical Assets. The Spot Check team verified the full list for Critical Cyber Assets associated with blackstart substations and transmission assets.

CIP-002-1 R3:
The violation posed a minimal risk to the reliability of the BPS and did not pose a serious or substantial risk to the reliability of the BPS because URE's Critical Cyber Assets were protected by CIP-005-1 and CIP-006-1, greatly reducing risk to the BES. The Critical Cyber Asset was redundant and any single device would not have had operational impacts. Finally, the scope of the violation was limited to assets single type of cyber asset.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

CIP-002-1 R1:
DURATION DATE(S) **7/1/08 through 12/3/10 (Mitigation Plan completion)**

CIP-002-1 R3:
DURATION DATE(S) **7/1/08 through 5/13/10 (Mitigation Plan completion)**

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

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

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

III. MITIGATION INFORMATION

CIP-002-1 R1:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-3669**
DATE SUBMITTED TO REGIONAL ENTITY	**9/22/10**
DATE ACCEPTED BY REGIONAL ENTITY	**4/29/11**
DATE APPROVED BY NERC	**6/10/11**
DATE PROVIDED TO FERC	**6/10/11**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**12/3/10**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**12/3/10**
DATE OF CERTIFICATION LETTER	**1/3/11**[6]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**12/3/10**
DATE OF VERIFICATION LETTER	**5/17/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**12/3/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE revised and updated the RBAM to provide criteria specific consideration for assets as required by R1.2.4 and R1.2.6. The revision to the RBAM considers NERC guidance as input in the revision of the RBAM and

[6] The Certification Document has a typographical error which lists the submittal and execution dates as being January 3, 2010.

procedures for application of the criteria in the RBAM. The RBAM includes criteria, and sufficient detail for application, aimed at ensuring a more consistent application of the RBAM to each of the asset types.

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)

- **Spreadsheet documents for the RBAM**
- **Asset identification methodology**

CIP-002-1 R3:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-2796**
DATE SUBMITTED TO REGIONAL ENTITY	**5/14/10**
DATE ACCEPTED BY REGIONAL ENTITY	**8/9/10**
DATE APPROVED BY NERC	**9/3/10**
DATE PROVIDED TO FERC	**9/3/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **5/13/10**[7]

DATE OF CERTIFICATION LETTER	**5/14/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**5/13/10**
DATE OF VERIFICATION LETTER	**8/30/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**5/13/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE revised its Critical Cyber Asset list to include the EMS operator consoles.

[7] The Settlement Agreement incorrectly lists the completion date as August 17, 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)

- **Revised list of its Critical Cyber Assets**
- **URE's Critical Cyber Asset identification procedure**
- **Screen shots supporting the active use of procedure**

EXHIBITS:

CIP-002-1 R1:

SOURCE DOCUMENT
WECC's Regional Determination of Alleged Violation Summary

MITIGATION PLAN
URE's Mitigation Plan MIT-08-3669

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

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

CIP-002-1 R3:

SOURCE DOCUMENT
WECC's Regional Determination of Alleged Violation Summary

MITIGATION PLAN
URE's Mitigation Plan MIT-08-2796

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-003-1 R1, R2, and R3

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment b.2

DISPOSITION OF VIOLATION

Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201001845	**URE_WECC20102086**
WECC201001846	**URE_WECC20102087**
WECC201001847	**URE_WECC20102088**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-003-1	**1**		**Medium**[1]	**N/A**[2]
CIP-003-1	**2**		**Medium**[3]	**N/A**
CIP-003-1	**3**		**Lower**	**N/A**

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

The purpose statement of CIP-003-1 provides in pertinent part: "Standard CIP-003 requires that Responsible Entities[4] have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009." Footnote added.

[1] CIP-003-1 R1 has a Medium Violation Risk Factor (VRF); R1.1, R1.2 and R1.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-003-1 R1 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the Medium VRF became effective. WECC originally assigned this violation a Lower VRF during its initial review and then determined that the Medium VRF was the appropriate VRF.

[2] At the time of the violations, no Violation Severity Levels (VSLs) were in effect for CIP-003-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[3] CIP-003-1 R2 has a Medium VRF; R2.1, R2.2 and R2.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-003-1 R2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-003-1 R2 was in effect from June 18, 2007 until January 27, 2009, when the Medium VRF became effective. WECC originally assigned this violation a Lower VRF during its initial review and then determined that the Medium VRF was the appropriate VRF.

[4] Within the text of Standard CIP-003, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

CIP-003-1 R1, R2, and R3 provide:

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

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

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

R2.1. The senior manager shall be identified by name, title, business phone, business address, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

VIOLATION DESCRIPTION

CIP-003-1 R1:
This violation was discovered during a WECC Spot Check of URE (Spot Check). URE failed to document a cyber security policy that addresses all requirements in Standards CIP-002 through CIP-009. Although URE identified the 13 Standard requirements, the WECC Spot Check Team determined that URE failed to include all 30 requirements in Standards CIP-002 through CIP-009 in its Cyber Security Policy.

CIP-003-1 R2:
During the Spot Check, WECC staff determined that URE failed to identify its designated senior manager's title, business phone, and business address during the period between August 26, 2008 and December 15, 2009 in violation of CIP-003-1 R2.1.

CIP-003-1 R3:
The Spot Check team found that URE had instances where it did not comply with its cyber security policy and did not document those exceptions to the URE's cyber security policy within thirty days of being approved by the senior manager. In total, URE had five documented exceptions covering 15 instances related to account and password management on URE's Critical Cyber Assets which required exceptions to the Cyber Security Policy.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

CIP-003-1 R1:[5]
This violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS) because URE had physical and electronic security around its Critical Cyber Assets. Also, even though URE's cyber security policy did not specifically reference all of the CIP standards which increases the possibility that protective measures will not be implemented correctly, URE's cyber security policy did address all the Reliability Standards for which URE as a "Table 1" entity was required to demonstrate compliance by July 1, 2008 but did not address all the requirements in Standards CIP-002 through CIP-009.

[5] WECC originally stated that the CIP-003-1 R1 violation posed a moderate risk to the BPS; however, after further review of the evidence and facts and circumstances, WECC determined that the risk to the BPS was minimal.

CIP-003-1 R2:
This violation posed a minimal and not serious or substantial risk to the reliability of the BPS because URE had a designated, appointed and documented Senior Manager responsible for overall compliance with the CIP standards; URE had only failed to document the title, business address, and business phone for a portion of the Spot Check period.[6]

CIP-003-1 R3:
This violation posed a minimal and not serious or substantial risk to the reliability of the BPS because the exceptions were not documented as exceptions to the cyber security policy related to account and password management on URE's Critical Cyber Assets. The exceptions themselves were documented but were not noted as an exception to the policy. The nature of the exceptions would not constitute a violation of any CIP standard, and the associated risks were substantially mitigated by the physical and electronic security around the Critical Cyber Assets .

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

CIP-003-1 R1:
DURATION DATE(S) **7/1/08 through 8/10/10 (Mitigation Plan completion)**

CIP-003-1 R2:
DURATION DATE(S) **7/1/08 through 12/16/09 (when the senior manager's title, business phone and address were included in the URE memorandum)**

CIP-003-1 R3:
DURATION DATE(S) **7/1/08 through 6/19/09[7] (Mitigation Plan completion)**

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

[6] The requirement for the business address and business phone number was eliminated from subsequent versions of this standard.
[7] Settlement Agreement incorrectly lists the end duration date as January 26, 2010.

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-003-1 R1:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-2534**
DATE SUBMITTED TO REGIONAL ENTITY	**5/14/10**
DATE ACCEPTED BY REGIONAL ENTITY	**5/20/10**
DATE APPROVED BY NERC	**6/14/10**
DATE PROVIDED TO FERC	**6/14/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **8/10/10**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **8/10/10**

DATE OF CERTIFICATION LETTER	**8/20/10**[8]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**8/10/10**
DATE OF VERIFICATION LETTER	**10/1/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**8/10/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
The URE information security manual Cyber Security Policy, containing the policies, standards and guidelines for CIP-003 R1 compliance, was updated and revised to reference more explicitly each NERC CIP-002 through CIP-009 requirement. The revised document was approved by the designated NERC CIP Senior Manager, and made available to personnel with access to NERC CIP assets/information. In addition to the modifications to policy statements within the information security manual document itself, a "cross walk" supplement was added to the information security manual to cross-

[8] The Settlement Agreement incorrectly lists the date of the Certification submittal as August 10, 2010.

reference explicitly each CIP requirement with the corresponding policy statement(s), thus demonstrating that the policy addresses each of the CIP requirements. The addition of the "cross walk" within the document provides documentation that the policy not only addresses all the requirements within CIP-002 through CIP-009, but also provides a mechanism to ensure the policy will continue to align with the CIP standards throughout each review and/or update.

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)

- **information security manual Cross-reference matrix which cross-references policies to standards**

CIP-003-1 R2:

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-2725**
DATE SUBMITTED TO REGIONAL ENTITY	**5/14/10**
DATE ACCEPTED BY REGIONAL ENTITY	**7/29/10**
DATE APPROVED BY NERC	**8/26/10**
DATE PROVIDED TO FERC	**8/26/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **12/16/09**

DATE OF CERTIFICATION LETTER	**5/14/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**12/16/09**
DATE OF VERIFICATION LETTER	**7/30/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**12/16/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE corrected the oversight when it appointed a new senior manager in August 2008 and documented the expansion of the memorandum to include the senior manager's title, business phone, and business address.

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)

- **Memorandum designating the URE CIP Senior Manager**

CIP-003-1 R3:
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-2726**
DATE SUBMITTED TO REGIONAL ENTITY	**5/14/10**
DATE ACCEPTED BY REGIONAL ENTITY	**7/29/10**
DATE APPROVED BY NERC	**8/26/10**
DATE PROVIDED TO FERC	**8/26/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **6/19/09**

DATE OF CERTIFICATION LETTER	**5/14/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**6/19/09**
DATE OF VERIFICATION LETTER	**7/30/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**6/19/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE documented the approval of exceptions by URE's designated Senior Manager.

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)

- **Attestation of the exception review**
- **Memo documenting approval of exceptions by URE's designated Senior Manager**
- **URE's information security exception form for operations**

EXHIBITS:

CIP-003-1 R1:

SOURCE DOCUMENT
WECC's Regional Determination of Alleged Violation Summary

MITIGATION PLAN
URE's Mitigation Plan MIT-08-2534

CERTIFICATION BY REGISTERED ENTITY
URE's Mitigation Plan Completion Certification

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

CIP-003-1 R2:

SOURCE DOCUMENT
WECC's Regional Determination of Alleged Violation Summary

MITIGATION PLAN
URE's Mitigation Plan MIT- 08-2725

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

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

CIP-003-1 R3:

SOURCE DOCUMENT
WECC's Regional Determination of Alleged Violation Summary

MITIGATION PLAN
URE's Mitigation Plan MIT- 08-2726

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007-1 R1

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment b.3

DISPOSITION OF VIOLATION

Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901818	**URE_WECC20092052**

I. VIOLATION INFORMATION

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

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

The purpose statement of CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities[3] to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009." (Footnote added.)

CIP-007-1 R1 provides:

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

[1] CIP-007-1 R1 and R1.1 each have a Medium Violation Risk Factor (VRF); R1.2 and R1.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-007-1 R1.1 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-007-1 R1.1 was in effect from June 18, 2007 until January 27, 2009, when the Medium VRF became effective.

[2] At the time of the violations, no Violation Severity Levels (VSLs) were in effect for CIP-007-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[3] Within the text of Standard CIP-007, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

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

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

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

VIOLATION DESCRIPTION

URE discovered the violation of CIP-007-1 R1 during a self-evaluation, and self-reported the violation a few months later. During the compliance Spot-Check, the WECC Spot Check team reviewed the Self-Report within its Spot Check review process. After reviewing the Self-Report and URE's Spot Check evidence, the WECC Spot Check established that URE's current cyber security test procedures were not implemented until May 14, 2009. Based on this discovery, the Spot Check team requested URE provide any test procedure documentation used between the December 12, 2008 violation discovery date and the implementation date of its current policy. URE's response indicated that no compliant test procedures were utilized between the effective date of the Standard and May 14, 2009, when URE implemented its current cyber security test procedures.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

The violation posed a moderate risk to the reliability of the bulk power system (BPS) because failing to have formal test procedures increases the possibility of undetected changes to existing security controls, thereby increasing vulnerability. The risk was not serious or substantial because URE conducted testing of new Cyber Assets and testing of significant changes to existing Cyber Assets, notwithstanding URE's failure to implement formal procedures complying with CIP-007-1 R1.

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) **7/1/08 through 5/14/09**[4] **(when URE implemented test procedures to satisfy the requirements of CIP-007-1)**

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-2735**
DATE SUBMITTED TO REGIONAL ENTITY	**5/14/10**
DATE ACCEPTED BY REGIONAL ENTITY	**8/17/10**
DATE APPROVED BY NERC	**8/27/10**
DATE PROVIDED TO FERC	**8/27/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **5/14/09**

[4] The Settlement Agreement incorrectly lists the duration of the violation as ending May 13, 2010.

DATE OF CERTIFICATION LETTER **5/14/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **5/14/09**

DATE OF VERIFICATION LETTER **8/18/10**[5]
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **5/14/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE revised its cyber security test procedures to include non-critical cyber assets, and conducted tests of all non-Critical Cyber Assets that have been added within the Electronic Security Perimeter.

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED, LIST EVIDENCE REVIEWED FOR COMPLETED MILESTONES)

- **URE EMS test procedures**

EXHIBITS:

SOURCE DOCUMENT
URE's Compliance Violation Self-Reporting Form
MITIGATION PLAN
URE's Mitigation Plan MIT-08-2735

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

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

[5] The Verification Letter is dated August 18, 2010 but the Settlement Agreement states that WECC notified URE on August 19, 2010 that it had accepted the Mitigation Plan and Certification of Mitigation Plan Completion.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-009-1 R1

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment b.4

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO. **WECC201001874**

REGIONAL ENTITY TRACKING NO. **URE_WECC20102134**

I. VIOLATION INFORMATION

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

CIP-009-1 R1 provides:

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

(Footnote added.)

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

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

VIOLATION DESCRIPTION

URE reported a violation of CIP-009-1 R1 through both the Self-Report and Self-Certification processes. URE failed to create a recovery plan for all of its Critical Cyber Assets, in violation of the Standard. Specifically, URE did not have a recovery plan for a generating station, a Critical Asset, until January 9, 2010.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

The violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS) because although URE did not have a documented plan for a generating station's facility, it was for only a period of nine days and even without a documented recovery plan, URE personnel were able to respond to events at a generating station that could activate a recovery plan and would have been able to recover Critical Cyber Assets. URE did have recovery plans for Critical Cyber Assets at other locations.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT	☐
SELF-CERTIFICATION	☒[3]
COMPLIANCE AUDIT	☐
COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK	☐
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

DURATION DATE(S) **1/1/10 through 1/9/10 (when URE created the generating station's Recovery Plan)**

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

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	☒

[3] URE reported this violation through both the Self-Report and Self-Certification processes. Because URE submitted both reports during the CIP Self-Certification submittal period, WECC determined the discovery method is Self-Certification.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2832**
DATE SUBMITTED TO REGIONAL ENTITY	**5/14/10**
DATE ACCEPTED BY REGIONAL ENTITY	**8/3/10**
DATE APPROVED BY NERC	**10/5/10**
DATE PROVIDED TO FERC	**10/6/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **1/9/10**

DATE OF CERTIFICATION LETTER	**5/14/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**1/9/10**
DATE OF VERIFICATION LETTER	**8/30/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**1/9/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE created a recovery plan for a generating station by January 9, 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)

- **the generating station's Recovery Plan**

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Certification for CIP-009-1 R1

MITIGATION PLAN
URE's Mitigation Plan MIT- 10-2832

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

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