NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

March 30, 2011

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Documents (Attachment i), 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-003-1 Requirement (R) 1 and R2; CIP-004-1 R2, R3 and R4; and CIP-007-1 R1 and R4. According to the Settlement Agreement, URE stipulates to the facts of the violations and has agreed to the assessed penalty of twenty seven thousand dollars ($27,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and

[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

conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC200901648, WECC200901649, WECC200901646, WECC200901647, WECC200901634, WECC200901635 and WECC200901636 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 July 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-595	WECC200901648	CIP-003-1	1/1.3	Lower[3]	7/1/08-6/11/09	27,000
	WECC200901649	CIP-003-1	2/2.1	Lower[4]	7/1/08-6/11/09	
	WECC200901646	CIP-004-1	2/2.1	Medium[5]	7/1/08-5/15/09	

[3] 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. In the context of this case, WECC determined the violation related to R1.3 and therefore a "Lower" VRF is appropriate.

[4] CIP-003-1 R2 has a "Medium" VRF; R2.1, R2.2, R2.3 and R2.4 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. In the context of this case, WECC determined the violation related to R2.1 and therefore a "Lower" VRF is appropriate.

[5] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" VRF; R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1, R2.2 and R2.2.4 "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-004-1 R2.1, R2.2 and R2.2.4 were in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRFs became effective. In the context of this case, WECC determined the violation related to R2.1 and therefore a "Medium" VRF is appropriate.

NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
	WECC200901647	CIP-004-1	3/3.2	Lower[6]	7/1/08-10/10/08	
	WECC200901634	CIP-004-1	4/4.1	Lower[7]	7/8/08-5/15/09	
	WECC200901635	CIP-007-1	1	Medium[8]	7/1/08-8/28/09	
	WECC200901636	CIP-007-1	4	Medium[9]	7/1/09-7/20/09	

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

CIP-003-1 R1 and R2 - OVERVIEW

During a Spot Check, WECC discovered violations of CIP-003-1 R1[10] and R2. WECC determined that URE, as a Responsible Entity,[11] could not provide evidence that URE's cyber security policy was reviewed and approved annually by the senior manager, as required by CIP-003-1 R1.3; and could not demonstrate that its senior manager was identified by business phone and business address prior to June 11, 2009, as required by CIP-003-1 R2.1.

CIP-004-1 R2, R3 and R4 - OVERVIEW

On June 18, 2009, URE discovered and on July 1, 2009, URE self-reported violations of CIP-004-1 R2, R3 and R4. WECC determined that URE, as a Responsible Entity, did not train at

[6] CIP-004-1 R3 has a "Medium" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-004-1 R3 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective. In the context of this case, WECC determined the violation related to R3.2 and therefore a "Lower" VRF is appropriate.

[7] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R4.2 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-004-1 R4.2 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[8] CIP-007-1 R1 and R1.1 each have a "Medium" VRF; R1.2 and R1.3 each have a "Lower" VRF. In the context of this case, WECC determined the violation related to R1.1 and R1.3 and therefore a "Medium" VRF is appropriate.

[9] When NERC filed VRFs it originally assigned CIP-007-1 R4. R4.1 and R4.2 "Lower" VRFs. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRFs and on February 2, 2009, the Commission approved the modified "Medium" VRFs. Therefore, the" Lower" VRFs for CIP-007-1 R4. R4.1, and R4.2 were in effect from June 18, 2007 until February 2, 2009, when the "Medium" VRFs became effective.

[10] The original Mitigation Plan and Certification of Completion for CIP-003-1 R1 addressed only the R1.2 sub-requirement, however WECC determined the violation was related to R1.3; URE addressed R1.3 in its revised Mitigation Plan.

[11] 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.

least two of its employees within 90 days of their being given authorized access to Critical Cyber Assets, as required by R2.1; did not update personnel risk assessments every seven years for at least 64 employees, as required by R3.2; and did not update its Critical Cyber Assets access list 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, as required by R4.1.[12]

CIP-007-1 R1 - OVERVIEW

On June 18, 2009, URE discovered and on July 1, 2009, URE self-reported a violation of CIP-007-1 R1. WECC determined that URE, as a Responsible Entity, did not have adequate cyber security test procedures, as required by R1.1; and did not document test results in all instances, as required by R1.3.

CIP-007-1 R4 - OVERVIEW

During a Spot Check, WECC discovered a violation of CIP-007-1 R4. WECC determined that URE, as a Responsible Entity, did not use anti-virus software or other malicious software (malware) prevention tools, where technically feasible, to detect, prevent, deter and mitigate the introduction, exposure, and propagation of malware on two of its Critical Cyber Assets.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[13]

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,[14] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2010. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a twenty seven thousand dollar ($27,000) 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 CIP-004-1 R2, R3 and R4 and CIP-007-1 R1 violations;[15]

[12] The precise number of instances when URE failed to update its access list is unknown, though its initial access list included 41 personnel, while its current access list included 137 personnel.
[13] *See* 18 C.F.R. § 39.7(d)(4).
[14] *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).
[15] WECC gave partial mitigating credit for these Self-Reports because they were submitted after the Notification of Spot Check sent by WECC on May 8, 2009. Also, additional aspects of the CIP-007-1 R1 violation were discovered at the Spot Check.

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), but the CIP-007-1 R1 and R4 violations did pose a moderate risk, as discussed in the Disposition Documents; and
7. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement. The NERC BOTCC agreed that the assessed penalty of twenty seven thousand dollars ($27,000) 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 part of this NOP are the following documents:

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

b) Record Documents for CIP-003-1 R1:

i. WECC's Determination of Alleged Violation Summary, included as Attachment b-1;[16]

ii. URE's Revised Mitigation Plan MIT-09-2258 submitted September 30, 2009 and Certification of Completion therein, included as Attachment b-2; and

iii. WECC's Verification of Mitigation Plan Completion dated March 11, 2010, included as Attachment b-3.

c) Record Documents for CIP-003-1 R2:

i. WECC's Determination of Alleged Violation Summary, included as Attachment c-1;

ii. URE's Mitigation Plan MIT-08-2259 submitted August 19, 2009, included as Attachment c-2;

iii. URE's Certification of Mitigation Plan Completion dated August 27, 2009, included as Attachment c-3; and

iv. WECC's Verification of Mitigation Plan Completion dated March 11, 2010, see Attachment b-3.

d) Record Documents for CIP-004-1 R2:

i. URE's Self-Report dated July 1, 2009, included as Attachment d-1;

ii. URE's Mitigation Plan MIT-08-2020 dated July 9, 2009 and submitted July 10, 2009, included as Attachment d-2;[17]

iii. URE's Certification of Mitigation Plan Completion dated August 27, 2009, included as Attachment d-3; and[18]

iv. WECC's Verification of Mitigation Plan Completion dated November 4, 2009, included as Attachment d-4.

e) Record Documents for CIP-004-1 R3:

i. URE's Self-Report dated July 1, 2009, included as Attachment e-1;[19]

ii. URE's Mitigation Plan MIT-08-2021 dated July 9, 2009 and submitted July 10, 2009, included as Attachment e-2;[20]

iii. URE's Certification of Mitigation Plan Completion dated August 27, 2009, included as Attachment e-3; and[21]

---

[16] The Determination of Alleged Violation Summary states that the violation beginning date was June 4, 2009 and that the Mitigation Plan was completed on June 10, 2009.
[17] The Settlement Agreement states that the Mitigation Plan was submitted on July 1, 2009. The Mitigation Plan states that the violation date is September 29, 2008.
[18] The Certification of Completion states that the Mitigation Plan was submitted on July 1, 2009.
[19] *See* n.17.
[20] The Settlement Agreement incorrectly states that the Mitigation Plan was submitted on July 1, 2009. The Mitigation Plan incorrectly states that the violation date is July 31, 2008.
[21] *See* n.18.

iv. WECC's Verification of Mitigation Plan Completion November 4, 2009, see Attachment d-4.

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

i. URE's Self-Report dated July 1, 2009, included as Attachment f-1;[22]

ii. URE's Mitigation Plan MIT-08-2003 dated July 9, 2009 and submitted July 10, 2009, included as Attachment f-2;[23]

iii. URE's Certification of Mitigation Plan Completion dated August 27, 2009, included as Attachment f-3; and[24]

iv. WECC's Verification of Mitigation Plan Completion dated November 4, 2009, see Attachment d-4.

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

i. URE's Self-Report dated July 8, 2009, included as Attachment g-1;[25]

ii. URE's Mitigation Plan MIT-08-2004 for CIP-007-1 R1 dated September 2, 2009 and submitted September 30, 2009, included as Attachment g-2;

iii. URE's Certification of Mitigation Plan Completion dated September 30, 2009, included as Attachment g-3; and

iv. WECC's Verification of Mitigation Plan Completion dated May 10, 2010, included as Attachment g-4.

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

i. WECC's Determination of Alleged Violation Summary, included as Attachment h-1;

ii. URE's Mitigation Plan MIT-09-2439 submitted September 2, 2009, included as Attachment h-2;[26]

iii. URE's Certification of Mitigation Plan Completion dated March 25, 2010, included as Attachment h-3; and

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

i) Disposition Document for Common Information, included as Attachment i:

i. Disposition Document for CIP-003-1 R1 and R2, included as Attachment i-1;

ii. Disposition Document for CIP-004-1 R2, R3 and R4, included as Attachment i-2; and

iii. Disposition Document for CIP-007-1 R1 and R4, included as Attachment i-3.

[22] *See* n.17.
[23] The Settlement Agreement incorrectly states that the Mitigation Plan was submitted on July 1, 2009.
[24] *See* n.18.
[25] The Settlement Agreement incorrectly states that the self-report was submitted on July 1, 2009.
[26] The Mitigation Plan incorrectly states that the violation was mitigated on July 13, 2009.

A Form of Notice Suitable for Publication[27]

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

[27] *See* 18 C.F.R. § 39.7(d)(6).

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net 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.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Davis Smith* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net davis.smith@nerc.net 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

Conclusion

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

Respectfully submitted,

/s/ *Rebecca J. Michael*
Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
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

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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment i

Disposition Document for Common Information

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS
Dated December 10, 2010

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-595**

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 ☒
Stipulates to the facts
ADMITS TO IT YES ☐
DOES NOT CONTEST IT (INCLUDING WITHIN 30 DAYS) YES ☐

WITH RESPECT TO THE ASSESSED PENALTY OR SANCTION, REGISTERED ENTITY

ACCEPTS IT/ DOES NOT CONTEST IT YES ☒

I. PENALTY INFORMATION

TOTAL ASSESSED PENALTY OR SANCTION OF **$27,000** FOR **SEVEN** VIOLATIONS OF A RELIABILITY STANDARD

(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 had a documented compliance program in place at the time of the violations that WECC considered a mitigating factor in determining the penalty.

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

(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
WECC gave partial mitigating credit for the CIP-004-1 R2, R3 and R4 and CIP-007-1 R1 Self-Reports because they were submitted after the Notification of Spot Check. Also, additional aspects of the CIP-007-1 R1 violation were discovered at the Spot Check.

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

NOTICE OF ALLEGED VIOLATION AND PROPOSED PENALTY OR SANCTION ISSUED
DATE: **11/11/09** OR N/A ☐

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **12/23/09** OR N/A ☐

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

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

REGISTERED ENTITY RESPONSE CONTESTED
FINDINGS ☐ PENALTY ☐ BOTH ☐ NO CONTEST ☒

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Disposition Document for CIP-003-1 R1 and R2

DISPOSITION OF VIOLATION
Dated December 10, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901648	**URE_WECC20091821**
WECC200901649	**URE_WECC20091822**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)[1]
CIP-003-1	**1**	**1.3**	**Lower[2]**	**N/A**
CIP-003-1	**2**	**2.1**	**Lower[3]**	**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] At the time of URE's violations, CIP-003-1 had Levels of Non-Compliance instead of Violation Severity Levels (VSLs). On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards, and the Commission approved the VSLs on March 18, 2010.
[2] 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. In the context of this case, WECC determined the violation related to R1.3 and therefore a "Lower" VRF is appropriate.
[3] CIP-003-1 R2 has a "Medium" VRF; R2.1, R2.2, R2.3 and R2.4 each have a "Lower" VRF. In the context of this case, WECC determined the violation related to R2.1 and therefore a "Lower" VRF is appropriate.
[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.

CIP-003-1 R1 and R2 provide in pertinent part:

> **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:**
>
> **…**
>
> **R1.3. 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….**

VIOLATION DESCRIPTION

During a Spot Check of URE, WECC discovered violations of CIP-003-1 R1 and R2. To determine compliance with CIP-003-1 R1, WECC subject matter experts (SMEs) reviewed two URE cyber security policies that were in effect during the compliance period dated May 14, 2008 and June 11, 2009. SMEs were unable to confirm that URE's cyber security policy was reviewed and approved annually by the assigned senior manager, as required by R1.3. Evidence available at the Spot Check indicated that URE's current senior manager was assigned to this position in April 2008, and that he reviewed and approved URE's current cyber security policy on June 11, 2009.

This assigned senior manager had reviewed, but not approved, the previous version of URE's cyber security policy dating back to May 2008. URE's Senior manager did initial the review and revision table at the back of the cyber security policy, and according to URE's Internal Compliance Program (ICP), this process constituted approval. Despite URE's process, the SMEs determined that the previous version of URE's cyber security policy had been approved by someone other than the assigned senior manager, in violation of R1.3.

SMEs determined that by an internal memorandum dated April 2008, URE assigned a senior manager over cyber security as required, but they also determined that this assignment did not identify the senior manager by business phone or business address, as required by R2.1. SMEs found that URE issued a reaffirming memorandum assigning the senior manager of cyber security and identifying him by business phone and business address on June 11, 2009. beyond. While URE believed that its published administrative documents, such as directories, which list the senior manager's business phone and business address, would meet the

documentation requirement, the WECC SMEs determined that not including the business phone and address of an indicated senior manager with overall responsibility for the entire compliance period was a violation of R2.1.

WECC Enforcement reviewed the findings of the SMEs and determined that URE had a violation of CIP-003-1 R1 and R2 because its cyber security policy was not reviewed and approved annually by the senior manager assigned pursuant to CIP-003-1 R2, as required by R1.3; and its senior manager was not identified by business phone and business address prior to June 11, 2009, as required by R2.1.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the CIP-003-1 R1 violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because URE had appointed a senior manager as required by R2 and that this Senior manager had reviewed and approved URE's cyber security policy as of June 11, 2009. In addition, WECC determined that the senior manager had reviewed previous versions of URE's cyber security policy dating back to May 2008. Furthermore, these previous versions had been approved by a responsible party at URE. URE was only in violation of this Standard because these previous versions were approved by someone other than the senior manager appointed under R2.

WECC determined that the CIP-003-1 R2 violation did not pose a serious or substantial risk to the reliability of the BPS because only the assigned senior manager's business phone and business address were missing in the designation.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) **7/1/08 (when the Standards became mandatory and enforceable for URE) through 6/11/09 (Mitigation Plan completion)**

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

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **R1: MIT-09-2258; R2: MIT-08-2259**
DATE SUBMITTED TO REGIONAL ENTITY **8/19/09**[5]
DATE ACCEPTED BY REGIONAL ENTITY **1/1/10**
DATE APPROVED BY NERC **1/13/10**
DATE PROVIDED TO FERC **1/13/10**

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 **N/A**
ACTUAL COMPLETION DATE **6/11/09**

DATE OF CERTIFICATION LETTER **R1: 9/30/09; R2: 8/27/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **R1: 6/16/09;**[6] **R2: 6/11/09**

DATE OF VERIFICATION LETTER **3/11/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **6/11/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
At the time of the Spot Check, URE had already mitigated the instant violation. To mitigate CIP-003-1 R1.3, URE stated that it specifically inserted words on the cover of its cyber security policy dated June 11, 2009 to demonstrate approval by its senior manager. To mitigate CIP-003-1 R2.1, URE stated that it issued an affirming memorandum on June 11, 2009, which identified URE's senior manager over cyber security and contained his business phone and business address.

[5] The original completed Mitigation Plan and Certification of Completion for CIP-003-1 R1 addressed only the R1.2 sub-requirement, however WECC determined the violation was related to R1.3. URE addressed R1.3 in its revised Mitigation Plan submitted to WECC on September 30, 2009.
[6] The completed Mitigation Plan for CIP-003-1 R1 incorrectly states the violation was mitigated June 16, 2009, the date the policy was posted to URE's intranet for access in order to address R1.2. WECC later deemed the violation applied only to R1.3 and was mitigated June 11, 2009, the date the policy was reviewed and updated.

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED, LIST EVIDENCE REVIEWED FOR COMPLETED MILESTONES)
URE provided two cyber security policy documents that were in effect during the compliance period and evidence of the senior manager designation at the time of the Spot Check.

EXHIBITS:

SOURCE DOCUMENT
WECC's Determination of Alleged Violation Summary for CIP-003-1 R1 showing a Spot Check
WECC's Determination of Alleged Violation Summary for CIP-003-1 R2 showing a Spot Check

MITIGATION PLAN
URE's Revised Mitigation Plan MIT-09-2258 for CIP-003-1 R1 submitted September 30, 2009 and Certification of Completion therein
URE's Mitigation Plan MIT-08-2259 for CIP-003-1 R2 submitted August 19, 2009

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-003-1 R2 dated August 27, 2009

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion for CIP-003-1 R1 and R2 dated March 11, 2010

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

DISPOSITION OF VIOLATION
Dated December 10, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901646	**URE_WECC20091819**
WECC200901647	**URE_WECC20091820**
WECC200901634	**URE_WECC20091807**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)[1]
CIP-004-1	**2**	**2.1**	**Medium[2]**	**N/A**
CIP-004-1	**3**	**3.2**	**Lower[3]**	**N/A**
CIP-004-1	**4**	**4.1**	**Lower[4]**	**N/A**

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

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

[1] At the time of URE's violations, CIP-004-1had Levels of Non-Compliance instead of Violation Severity Levels (VSLs). On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards, and the Commission approved the VSLs on March 18, 2010.
[2] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" Violation Risk Factor (VRF); R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective. In the context of this case, WECC determined the violation related to R2.1 and therefore a "Medium" VRF is appropriate.
[3] CIP-004-1 R3 has a "Medium" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-004-1 R3 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective. In the context of this case, WECC determined the violation related to R3.2 and therefore a "Lower" VRF is appropriate.
[4] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF.

CIP-004-1 R2, R3 and R4 provide in pertinent part:

> **R2. Training — The Responsible Entity[5] shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary. (Footnote added.)**
>
> > **R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.**
> >
> > **…**
>
> **R3. Personnel Risk Assessment — The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:**
>
> > **…**
> >
> > **R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.**
> >
> > **…**
>
> **R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.**
>
> > **R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.**

[5] Within the text of Standard CIP-004, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC and Regional Reliability Organizations.

VIOLATION DESCRIPTION

On June 18, 2009, URE discovered, and on July 1, 2009, URE self-reported, violations of CIP-004-1 R2, R3 and R4 to WECC. First, URE stated that it had instituted a cyber security training program, but two of its employees had not been trained within 90 days of being given authorized access to Critical Cyber Assets, as required by R2.1. Second, URE stated that it had instituted a personnel risk assessment program as required by R3, but URE was unable to update all personnel risk assessments for personnel who did not have background checks conducted within the last seven years, as required by R3.2. Third, URE stated that it had created a list of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as required by R4, but this list was not consistently updated when changes in access rights to Critical Cyber Assets were made, as required by R4.1.

During the Spot Check of URE, WECC subject matter experts (SMEs) reviewed the self-reported violations. First, SMEs determined that two individuals had not been trained within 90 days of being given authorized access to Critical Cyber Assets and found that URE could not present evidence demonstrating the date these two individuals were given access to Critical Cyber Assets. Second, SMEs found that URE screened all employees by October 2008 and determined that several URE employees with authorized access to Critical Cyber Assets did not have background checks conducted within the seven years prior to October 2008. Third, SMEs found that URE's early access lists identified personnel who had access to Critical Cyber Assets, but URE's current access list identified additional personnel having access to Critical Cyber Assets. In addition, WECC SMEs determined that there were several instances where persons were identified by position title rather than by individual name. Based on the evidence URE provided, WECC was unable to determine the precise number of non-compliance instances.

WECC Enforcement reviewed the findings of the SMEs and determined that URE did not train at least two of its employees within 90 days of their being given authorized access to Critical Cyber Assets, as required by R2.1; did not update personnel risk assessments every seven years for some employees, as required by R3.2; and did not update its Critical Cyber Assets access list in many instances 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, as required by R4.1.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the CIP-004-1 R2 violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because all but two URE employees did receive the required training within 90 days.

WECC determined that the CIP-004-1 R3 violation did not pose a serious or substantial risk to the reliability of the BPS because the employees who did not have updated personnel risk assessments did receive background checks when initially hired.

WECC determined that the CIP-004-1 R4 violation did not pose a serious or substantial risk to the reliability of the BPS because the security provided by an updated access list is in addition to security provided by physical and electronic controls established in accordance with CIP-005-1 and CIP-006-1, which serves as the primary barrier to unauthorized access to Critical Cyber Assets. In this case, URE's violation related only to the maintenance of an access list which correctly identified personnel who have been given authorized access to Critical Cyber Assets through these physical and electronic security controls. In addition, this violation did not represent a failure to remove individuals from the list who no longer have authorized access; such a failure would pose a greater risk to the reliability of the BPS than did URE's failure to add authorized individuals to its access list. WECC SMEs found that URE's early access lists identified personnel with access to CCAs. However, URE's current access list identified additional personnel having access to CCAs. In addition, WECC SMEs determined that there were several instances where persons were identified by position title rather than by individual name. URE's access list was not updated within seven calendar days of any change of personnel with access to CCAs as required by R4.1, from July 8, 2008 until May 15, 2009.

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: 7/1/08 (when the Standard became mandatory and enforceable for URE) through 5/15/09 (Mitigation Plan completion)**

R3: 7/1/08 (when the Standard became mandatory and enforceable for URE) through 10/10/08 (Mitigation Plan completion)
R4: 7/8/08 (first due date the Critical Cyber Assets access list should have been updated) through 5/15/09 (Mitigation Plan completion)

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

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **R2: MIT-08-2020;[6] R3: MIT-08-2021;[7] R4: MIT-08-2003[8]**
DATE SUBMITTED TO REGIONAL ENTITY **dated 7/9/09 and submitted 7/10/09**
DATE ACCEPTED BY REGIONAL ENTITY **7/9/09[9]**
DATE APPROVED BY NERC **R2: 9/25/09; R3: 10/12/09; R4: 10/12/09**
DATE PROVIDED TO FERC **R2: 9/25/09; R3: 10/12/09; R4: 10/12/09**

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

URE originally submitted its completed Mitigation Plans for the CIP-004-1 R2, R3 and R4 violations on July 1, 2009, with the Self-Reports. These versions of the Mitigation Plans were reviewed during the Spot Check and revised to provide additional information.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **R2: 5/15/09; R3: 10/10/08; R4: 5/15/09;**

[6] The Settlement Agreement states that the Mitigation Plan was submitted on July 1, 2009. The Mitigation Plan incorrectly states that the violation date is September 29, 2008.
[7] The Settlement Agreement states that the Mitigation Plan was submitted on July 1, 2009. The Mitigation Plan incorrectly states that the violation date is July 31, 2008.
[8] The Settlement Agreement states that the Mitigation Plan was submitted on July 1, 2009.
[9] WECC accepted the Mitigation Plan during an audit prior to URE's formal submission of the Mitigation Plan via the WECC portal on July 10, 2009.

DATE OF CERTIFICATION LETTER **8/27/09**[10]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **R2: 5/15/09 R3: 10/10/08 R4: 5/15/09**

DATE OF VERIFICATION LETTER **11/4/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **R2: 5/15/09; R3: 10/10/08; R4: 5/15/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
Based on the evidence reviewed, the SMEs did not identify non-compliance by URE with CIP-004-1 R2, R3 and R4 at the time of the Spot Check.

To mitigate CIP-004-1 R2.1, URE took the following actions:
URE implemented procedural and organizational controls, including the authorization of a senior manager to immediately revoke access privileges in cases of incomplete training. URE stated that by May 15, 2009, all individuals who had not received required training had their access revoked; all personnel that now have access to Critical Cyber Assets had received required training; URE developed a document which outlined the process that must be taken before access is granted to employees and contractors; URE developed a worksheet that must be completed and signed by all appropriate parties before personnel are placed on its list of personnel with access to Critical Cyber Assets; personnel can only be given access if their name appears on this list; a URE senior manager is the only person who can grant access, and does so only after all applicable requirements have been met; and URE electronically tracks training for all personnel with access.

To mitigate CIP-004-1 R3.2, URE took the following actions:
URE completed a personnel risk assessment consisting of identity verification and a 7-year background check for all employees having authorized access to Critical Cyber Assets on October 2008. URE updated its personnel risk assessment program and implemented procedural controls to ensure that all personnel and contractors have personnel risk assessments completed before hiring. If background checks reveal relevant information, documentation goes to an assistant manager for approval to complete the personnel risk assessment process. Before individuals receive authorized access to Critical Cyber Assets a worksheet must be completed. This worksheet has a data field for personnel risk assessments; access will not be granted if the date in this field is more than 7 years old. Upon receiving access, the individual and his or her personnel risk assessment date are noted on URE's list of employees with access to Critical Cyber Assets. This list tracks the personnel risk assessments of all employees with authorized access to Critical Cyber

[10] The Certification of Completions incorrectly state that the Mitigation Plans were submitted on July 1, 2009.

Assets. If an individual is out of compliance with the personnel risk assessment requirement, a senior manager revokes access immediately and notifies the individual.

To mitigate CIP-004-1 R4.1, URE took the following actions:
URE audited its list of personnel with access and authorization against its physical and electronic access controls. Only those individuals that were on this list were then allowed authorized access to Critical Cyber Assets and the specific access granted was made consistent with the access privileges documented on the list by May 15, 2009. In addition, URE implemented strong procedural controls to ensure that all personnel and contractors having authorized access to Critical Cyber Assets were first documented on the list before such access was granted. Specifically, URE developed a document which outlines the process that must take place before access is granted to personnel and contractors. This document requires a worksheet to be completed and signed by all appropriate parties before personnel are placed on the list or when access privileges need revision. Personnel can only be given authorized access if their name appears on the List and a Cyber Security acts as a single point of enforcement and control since he is now the only person who can authorize access into CIP-related areas and he does so only after satisfying himself that the appropriate documentation is maintained and that the personnel are compliant will all applicable requirements before granting access.

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED, LIST EVIDENCE REVIEWED FOR COMPLETED MILESTONES)
URE provided the evidence in support of its completion of the Mitigation Plans at the time of the Spot Check.

At the Spot Check, WECC reviewed URE's Cyber Security personnel and training documents; and URE's process for assigning, validating and authorizing access privileges

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-004-1 R2 dated July 1, 2009
URE's Self-Report for CIP-004-1 R3 dated July 1, 2009
URE's Self-Report for CIP-004-1 R4 dated July 1, 2009

MITIGATION PLAN
URE's Mitigation Plan MIT-08-2020 for CIP-004-1 R2 dated July 9, 2009 and submitted July 10, 2009
URE's Mitigation Plan MIT-08-2021 for CIP-004-1 R3 dated July 9, 2009 and submitted July 10, 2009
URE's Mitigation Plan MIT-08-2003 for CIP-004-1 R4 dated July 9, 2009 and submitted July 10, 2009

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-004-1 R2 dated August 27, 2009
URE's Certification of Mitigation Plan Completion for CIP-004-1 R3 dated August 27, 2009
URE's Certification of Mitigation Plan Completion for CIP-004-1 R4 dated August 27, 2009

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion for CIP-004-1 R2, R3 and R4 dated November 4, 2009

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Disposition Document for CIP-007-1 R1 and R4

DISPOSITION OF VIOLATION
Dated December 10, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901635	**URE_WECC20091808**
WECC200901636	**URE_WECC20091809**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)[1]
CIP-007-1	**1**	**1.1, 1.3**	**Medium[2]**	**N/A**
CIP-007-1	**4**		**Medium[3]**	**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[4] 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 and R4 provide in pertinent part:

> **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**

[1] At the time of URE's violations, CIP-007-1had Levels of Non-Compliance instead of Violation Severity Levels (VSLs). On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards, and the Commission approved the VSLs on March 18, 2010.
[2] CIP-007-1 R1 and R1.1 each have a "Medium" VRF; R1.2 and R1.3 each have a "Lower" VRF. In the context of this case, WECC determined the violation related to R1.1 and R1.3 and therefore a "Medium" VRF is appropriate.
[3] When NERC filed VRFs it originally assigned CIP-007-1 R4 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on February 2, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-007-1 R4 was in effect from June 18, 2007 until February 2, 2009, when the "Medium" VRF became effective.
[4] 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.

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.

…

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.

…

VIOLATION DESCRIPTION

On June 18, 2009, URE discovered and on July 8, 2009, URE self-reported a violation of CIP-007-1 R1 to WECC. URE stated that it had tested all new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter per the Standard, except testing was not documented in all cases, as required by R1.3.

During the Spot Check of URE, WECC subject matter experts (SMEs) reviewed the self-reported violation. SMEs interviewed URE personnel and determined that URE was in violation of R1.3 as described in URE's Self-Report. In addition, SMEs reviewed a URE system security management document. SMEs found that although the document did address test procedures in general, it did not specifically address "cyber security test procedures," as required by R1.1. Specifically, SMEs determined that these procedures did not consider the effects of new Cyber Assets

and significant changes to existing Cyber Assets within the Electronic Security Perimeter on the existing security controls for the particular Critical Cyber Asset being tested.

Also during the Spot Check of URE, WECC discovered a violation of CIP-007-1 R4. SMEs interviewed URE personnel and determined that two Critical Cyber Assets were tested and found to be unstable with the URE standard anti-virus software. Therefore URE did not install the standard anti-virus software on the referenced Critical Cyber Assets.[5]

WECC Enforcement reviewed the findings of the SMEs and determined that URE did not have adequate cyber security test procedures, as required by R1.1; did not document test results in all instances, as required by R1.3; and did not use anti-virus software or other malware prevention tools, where technically feasible, to detect, prevent, deter and mitigate the introduction, exposure, and propagation of malware on two the Critical Cyber Assets, as required by R4.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the CIP-007-1 R1 violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), because URE had documented its Critical Cyber Assets and did have cyber security testing procedures. WECC did find that the violation did pose a moderate risk because these testing procedures did not properly address cyber security controls. Due to URE's failure to have adequate testing procedures, it could not assure that proposed changes to Critical Cyber Assets were being properly tested. This resulted in an increased probability that implementation of changes to Critical Cyber Assets could weaken or make inoperable existing cyber security controls.

WECC determined that the CIP-007-1 R4 violation did not pose a serious or substantial risk to the reliability of the BPS, but did pose a moderate risk. URE's failure to verify that two of its Critical Cyber Assets were protected by alternate anti-virus software is a failure to ensure that these Critical Cyber Assets had been protected to the greatest degree possible. Nevertheless, the risk was mitigated because URE's Critical Cyber Assets were protected by its primary anti-virus protection software.

[5] At the time of the Spot Check, URE explained that only the URE standard anti-virus software package was tested, and no other options were considered other than a newer package of URE's current anti-virus software. URE noted that NERC guidance regarding technical feasibility was not issued in a compliance process bulletin until July 1, 2009 when NERC issued its *Interim Approach to Technical Feasibility Exceptions*. In addition, there was no published method or form to submit technical feasibility exceptions to the regions prior to URE's Spot Check. SMEs determined that for an entity to be exempted from compliance with this Standard, a reasonable solution to address the requirements of the Standard must not exist. WECC does not grant exceptions based on an entity's determination that its standard practices were infeasible.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT **(R1)**	☒[6]
SELF-CERTIFICATION	☐
COMPLIANCE AUDIT	☐
COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK **(R4)**	☒
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

DURATION DATE(S) **R1: 7/1/08 (when the Standard became mandatory and enforceable for URE) through 8/28/09 (Mitigation Plan completion)**
R4: 7/1/09 (when the Standard became mandatory and enforceable for URE) through 7/20/09 (Mitigation Plan completion)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **R1:7/8/09; R4: Spot Check**

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **R1: MIT-08-2004; R4: MIT-09-2439**[7]
DATE SUBMITTED TO REGIONAL ENTITY **9/2/09**[8]
DATE ACCEPTED BY REGIONAL ENTITY **R1: 7/6/09 R4: 3/22/10**
DATE APPROVED BY NERC **R1: 9/25/09 R4: 4/19/10**
DATE PROVIDED TO FERC **R1: 9/25/09 R4: 4/19/10**

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

URE originally submitted its completed Mitigation Plan for CIP-007-1 R1 on July 1, 2009. This version of the Mitigation Plan was reviewed during the Spot Check. This version certified completion on May 13, 2009 and was

[6] The Settlement Agreement incorrectly states that the self-report was submitted on July 1, 2009.
[7] The Mitigation Plan incorrectly states that the violation was mitigated on July 13, 2009.
[8] The revised Mitigation Plan for CIP-007-1 R1 is dated September 2, 2009, but was submitted to WECC September 30, 2009.

based on only non-compliance with the R1.3 sub-requirement. The subsequent version of the Mitigation Plan addressed non-compliance with the R1.1 sub-requirement.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE
R1: 8/28/09; R4: 7/20/09[9]

DATE OF CERTIFICATION LETTER
R1: 9/30/09; R4: 3/25/10
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF
R1: 8/28/09; R4: 7/20/09

DATE OF VERIFICATION LETTER
R1: 5/10/10; R4: 4/1/10
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF
R1: 8/28/09; R4: 7/20/09

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
To mitigate CIP-007-1 R1.3, URE took the following actions:
URE reinforced its awareness and training activities to ensure that the testing documentation needs are well understood; URE created a dedicated, standardized form to capture the execution of all testing activities; URE made its technicians aware of this form and that they are responsible for completing this form as required by URE system security management procedures; URE added additional provisions to these procedures to clarify the applicability and activity scopes of the testing provisions; URE improved the tracking aspect of all patches and version upgrades to ensure that such testing can take place in a timely manner; and URE implemented an automated systems to ensure accuracy of records in the tracking and testing of assets.

To mitigate CIP-007-1 R1.1, URE modified its test procedures in its system security management document to explicitly include a subsection that addressed the testing of the cyber security controls of the in-scope Cyber Asset that has gone through a significant change per the Standard.

To mitigate CIP-007-1 R4, URE conducted testing of additional commercial anti-virus software products, and successfully tested and installed alternate

[9] The completed Mitigation Plan for CIP-007-1 R4 incorrectly states the violation was mitigated July 13, 2009.

anti-virus software on two of the Critical Cyber Assets. The installation process was completed on July 20, 2009.

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED, LIST EVIDENCE REVIEWED FOR COMPLETED MILESTONES)
URE provided the evidence in support of its completion of the Mitigation Plan for R1 at the time of the Spot Check. In addition, to demonstrate compliance with R1.1, URE provided WECC with a copy of system security management.

For R4, WECC reviewed documentation showing that testing and installation of all anti-virus software on two of the Critical Cyber Assets was successfully completed.

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R1 dated July 8, 2009
WECC's Determination of Alleged Violation Summary for CIP-007-1 R4

MITIGATION PLAN
URE's Mitigation Plan MIT-08-2004 for CIP-007-1 R1 dated September 2, 2009 and submitted September 30, 2009
URE's Mitigation Plan MIT-09-2439 for CIP-007-1 R4 submitted September 2, 2009

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-007-1 R1 dated September 30, 2009
URE's Certification of Mitigation Plan Completion for CIP-007-1 R4 dated March 25, 2010

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion for CIP-007-1 R1 dated May 10, 2010
WECC's Verification of Mitigation Plan Completion for CIP-007-1 R4 dated April 1, 2010