PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

June 29, 2011

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Disposition Documents attached hereto (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 URE does not dispute the violations of CIP-004-1 Requirement (R) 2, CIP-004-1 R3, CIP-005-1 R2, CIP-005-1 R3, CIP-007-1 R2 and CIP-007-1 R8 and the assessed three hundred eighty-one thousand six hundred dollar ($381,600) penalty. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201002288, WECC200902079, WECC201002082, WECC201002088, WECC201002080 and WECC200902081 are Confirmed Violations, as that term is defined in the NERC Rules of Procedure and the CMEP.

[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

Statement of Findings Underlying the Violations

This NOP incorporates the findings and justifications reported in the Notice of Confirmed Violation and Proposed Penalty or Sanction (NOCV) issued on December 16, 2010, by Western Electricity Coordinating Council (WECC), as described in the Disposition Documents. The details of the findings and the basis for the penalty are set forth in the Disposition Documents. This NOP filing contains the basis for approval of this NOP by the NERC Board of Trustees Compliance Committee (BOTCC). In accordance with Section 39.7 of the Commission's Regulations, 18 C.F.R. § 39.7, NERC provides the following summary table identifying each violation of a Reliability Standard at issue in this NOP.

NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
NOC-754	WECC201002288	CIP-004-1	2	Lower[3]	12/30/09-11/1/10	381,600
	WECC200902079	CIP-004-1	3	Medium[4]	7/1/09-3/19/10	
	WECC201002082	CIP-005-1	2	Medium[5]	7/1/09-3/23/10	
	WECC201002088	CIP-005-1	3	Medium	7/1/09-4/30/10	
	WECC201002080	CIP-007-1	2	Medium	7/1/09-12/15/10	
	WECC200902081	CIP-007-1	8	Medium[6]	7/1/09-12/15/10	

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

CIP-004-1 R2 - OVERVIEW

Over the course of its review, with a WECC subject matter expert, of documentation related to URE's Self-Report of a CIP-004-1 R3 violation, detailed below, URE submitted a Self-Report. WECC determined that URE failed to maintain documentation that it conducted training at least annually, including the date the training was completed and attendance records for four employees as required by CIP-004-1 R2.3.

CIP-004-1 R3 - OVERVIEW

This violation was discovered during an internal review, and URE submitted a Self-Report to WECC. WECC determined that URE failed to conduct several Personnel Risk Assessments

[3] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" Violation Risk Factor (VRF); R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. In the context of this case, WECC determined the violation related to R2.3, and therefore a "Lower" VRF is appropriate.
[4] CIP-004-1 R3 has a "Medium" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF.
[5] CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" VRF; R2.5 and its sub-requirements and R2.6 each have a "Lower" VRF.
[6] CIP-007-1 R8 and R8.1 each have a "Lower" VRF; R8.2, R8.3 and R8.4 each have a "Medium" VRF. In the context of this case, WECC determined the violation related to R8.2, and therefore a "Medium" VRF is appropriate.

(PRAs) pursuant to URE's program within thirty days of its employees and contractors being granted authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) as required by R3. This represented approximately 9 percent of URE's employees or contractors which had access to CCAs without having a completed PRA.

CIP-005-1 R2 - OVERVIEW

URE submitted a Self-Report addressing CIP-005-1 R2 and then submitted its Self-Certification to WECC.[7] WECC determined that URE failed to implement organizational processes and technical and procedural mechanisms for control of electronic access at all of URE's electronic access points to its Electronic Security Perimeters (ESPs) as required by R2.

CIP-005-1 R3 - OVERVIEW

URE submitted a Self-Report addressing CIP-005-1 R3 and then submitted its Self-Certification to WECC.[8] WECC determined that URE failed to implement an electronic or manual process for monitoring and logging access at access points to the ESP twenty-four hours a day, seven days a week as required by R3.

CIP-007-1 R2 - OVERVIEW

On January 19, 2010, URE submitted a Self-Report addressing CIP-007-1 R2 and then submitted its Self-Certification to WECC on January 28, 2010.[9] WECC determined that URE, as a Responsible Entity, did not conduct and document a baseline scan for ports and services and could not establish and document a process to ensure that only those ports and services required for normal and emergency operations were enabled as required by R2.

CIP-007-1 R8 - OVERVIEW

The CIP-007-1 R8 violation was discovered during an internal review, and URE submitted a Self-Report to WECC. WECC determined that URE failed to conduct a review to verify that only ports and services required for operation of the Cyber Assets within URE's ESP were enabled as required by R8.2.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[10]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[11] the NERC BOTCC reviewed the NOCV and supporting documentation on May 9,

[7] Although URE self-reported this violation, because URE self-reported during the Self-Certification submission period, the discovery method for this violation is classified as Self-Certification.
[8] *Id*.
[9] *Id*.
[10] *See* 18 C.F.R § 39.7(d)(4).
[11] *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).

2011. The NERC BOTCC approved the NOCV and the assessment of a three hundred eighty-one thousand six hundred dollar ($381,600) financial penalty against URE based upon WECC's findings and determinations, the NERC BOTCC's review of the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. the violations constituted URE's first violation of the subject NERC Reliability Standards;
2. URE self-reported three violations (CIP-004-1 R2,[12] CIP-004-1 R3 and CIP-007-1 R8) and the other three violations were discovered during URE's self-certification submission period;
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 posed a moderate risk, except for CIP-004-1 R2 which posed a minimal risk, and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), as discussed in the Disposition Documents; and
7. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC believes that the assessed penalty of three hundred eighty-one thousand six hundred dollars ($381,600) 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 the Commission, or, if the Commission decides to review the penalty, upon final determination by the Commission.

Request for Confidential Treatment

Information in and certain attachments to the instant 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.

[12] URE self-reported CIP-004-1 R2 after an inquiry thus only receiving partial mitigating credit.

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) URE's Response to the Notice of Alleged Violation and Proposed Penalty or Sanction dated December 14, 2010, included as Attachment a;[13]

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

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

   ii. Disposition Document for CIP-005-1 R2 and R3, included as Attachment b-2; and

   iii. Disposition Document for CIP-007-1 R2 and R8, included as Attachment b-3.

c) Record Documents for CIP-004-1 R2, included as Attachment c:

   i. URE's Self-Report for CIP-004-1 R2, included as Attachment c-1;

   ii. URE's Mitigation Plan MIT-09-3121, 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.

d) Record Documents for CIP-004-1 R3, included as Attachment d:

   i. URE's Self-Report for CIP-004-1 R3, included as Attachment d-1;

   ii. URE's Mitigation Plan MIT-09-2886, 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.

e) Record Documents for CIP-005-1 R2, included as Attachment e:

   i. URE's Self-Certification for CIP-005-1 R2, included as Attachment e-1;

   ii. URE's Mitigation Plan MIT-09-2894, included as Attachment e-2;

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

[13] The Notice of Alleged Violation and Proposed Penalty or Sanction document includes a typographical error and the CIP-002 reference should be CIP-004.

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

f) Record Documents for CIP-005-1 R3, included as Attachment f:

i. URE's Self-Certification for CIP-005-1 R3, *see* Attachment e-1;

ii. URE's Mitigation Plan MIT-09-2895, included as Attachment f-1;

iii. URE's Certification of Mitigation Plan Completion, included as Attachment f-2; and

iv. WECC's Verification of Mitigation Plan Completion, included as Attachment f-3.

g) Record Documents for CIP-007-1 R2 and CIP-007-1 R8, included as Attachment g:

i. URE's Self-Certification for CIP-007-1 R2, *see* Attachment e-1;

ii. URE's Self-Report for CIP-007-1 R8, included as Attachment g-1;

iii. URE's Mitigation Plan MIT-09-2868, included as Attachment g-2;

iv. URE's Certification of Mitigation Plan Completion, included as Attachment g-3; and

v. WECC's Verification of Mitigation Plan Completion, included as Attachment g-4.

A Form of Notice Suitable for Publication[14]

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

[14] *See* 18 C.F.R. § 39.7(d)(6).

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 713-9598 (801) 582-3918 – facsimile Mark@wecc.biz Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6855 (801) 883-6894 – facsimile CWhite@wecc.biz Sandy Mooy* Associate General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7658 (801) 883-6894 – facsimile SMooy@wecc.biz	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net Christopher Luras* Manager of Compliance Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this 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 Corporate and Regulatory Matters
Sonia C. Mendonça
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

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 May 9, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-754**

REGIONAL ENTITY
Western Electricity Coordinating Council (WECC)

IS THERE A SETTLEMENT AGREEMENT YES ☐ NO ☒

WITH RESPECT TO THE VIOLATION(S), REGISTERED ENTITY

NEITHER ADMITS NOR DENIES IT (SETTLEMENT ONLY) YES ☐
ADMITS TO IT YES ☐
DOES NOT CONTEST IT (INCLUDING WITHIN 30 DAYS) YES ☒

WITH RESPECT TO THE ASSESSED PENALTY OR SANCTION, REGISTERED ENTITY

ACCEPTS IT/ DOES NOT CONTEST IT YES ☒

I. PENALTY INFORMATION

TOTAL ASSESSED PENALTY OR SANCTION OF **$381,600** FOR **SIX** VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

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

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ NO ☐ UNDETERMINED ☐
EXPLAIN
URE had an internal compliance program (ICP) at the time of the violations which 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

(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: **11/16/10** OR N/A ☐

SETTLEMENT DISCUSSIONS COMMENCED
DATE: OR N/A ☒

NOTICE OF CONFIRMED VIOLATION ISSUED
DATE: **12/16/10** OR N/A ☐

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

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

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-1 R2 and R3

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

DISPOSITION OF VIOLATION
Dated May 9, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002288	**WECC2010-610540**
WECC200902079	**WECC2010-609982**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**2**	**2.3**	**Lower**[1]	**Severe**[2]
CIP-004-1	**3**		**Medium**[3]	**Severe**

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

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

CIP-004-1 R2 provides in pertinent part:

> **R2. Training — The Responsible Entity[4] 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.**
> **…**

[1] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" Violation Risk Factor (VRF); R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. In the context of this case, WECC determined the violation related to R2.3, and therefore a "Lower" VRF is appropriate
[2] WECC assessed the "Severe" VSL based on the VSL Matrix for R2.3.
[3] CIP-004-1 R3 has a "Medium" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF.
[4] 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.

> **R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.**

CIP-004-1 R3 provides:

> **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:**
>
> > **R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.**
> >
> > **R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.**
> >
> > **R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.**

(Footnote added.)

VIOLATION DESCRIPTION

URE discovered a violation of CIP-004-1 R3 during an internal review and submitted a Self-Report to WECC. According to the Self-Report, 18 URE employees or contractors were granted electronic access to Critical Cyber Assets (CCAs) before completing personnel risk assessments (PRAs) and/or training. URE disabled electronic access to CCAs for those identified individuals upon this discovery and stated the inappropriate access occurred while URE was implementing a new automated reporting process during the third quarter of 2009.

URE also stated that there was a reporting gap associated with the manual process used earlier in 2009 to validate background checks and training compliance.

A WECC subject matter expert (SME) reviewed the Self-Report and determined that URE had a PRA program in effect at the time of, and prior to, the Self-Report. To make this determination, the SME reviewed URE's Personnel Risk Assessment procedures. The SME conducted a phone interview with a URE Manager. The SME noted that URE stated in the Self-Report that PRAs "and/or training" were not provided to personnel. The SME further noted that training is related to a different requirement within CIP-004-1 and, URE subsequently self-reported a violation of CIP-004-1 R2. In this Self-Report, URE stated that four individuals having electronic access did not have current training at the time of the December 30, 2009 CIP-004-1 R3 Self-Report.[5]

During the CIP-004-1 R3 Self-Report review, including and following the phone interview, the SME determined 24 URE personnel had access to CCAs before getting a PRA completed. Following submittal of its Self-Report, URE further reviewed its card holders and determined that an additional 177 employees and 29 contractors had physical access to Critical Assets (*e.g.*, card key to substations) without getting a PRA completed. URE revoked access for these individuals immediately upon discovering the individuals did not have completed PRAs. The SME determined that approximately 9 percent of URE personnel with authorized cyber or authorized unescorted physical or logical access to CCAs did not have a completed PRA. Therefore, the SME determined that URE did not ensure that a PRA was conducted pursuant to URE's PRA program within 30 days of such personnel being granted authorized cyber or authorized unescorted physical access to CCAs in violation of CIP-004-1 R3. The SME forwarded this Self-Report and its findings to WECC Enforcement.

During the CIP-004-1 R2 Self-Report review, including and following the phone interview on September 1, 2010, a URE Manager stated that four URE employees, with physical access to CCAs (specifically substations), had not received URE's annual cyber security training. Therefore, the SME determined URE did not maintain documentation that URE conducted such training annually, including the date the four employees completed the training and their attendance records in violation of CIP-004-1 R2.3. The SME forwarded this Self-Report and its findings to WECC Enforcement.

WECC Enforcement determined URE failed to conduct a PRA pursuant to URE's program within thirty days of its personnel (as outlined above) being granted

[5] According to the CIP-004-1 R2 Mitigation Plan, URE was not aware that four individuals did not have current training until the two separate databases were combined and both PRA and training records were updated. This discrepancy was discovered during WECC's review of the CIP-004-1 R3 Self-Report and Mitigation Plan by WECC, and URE agreed to self-report the violation of CIP-004-1 R2. WECC applied partial Self-Report credit because the violation was self-reported after the WECC inquiry.

authorized cyber or authorized unescorted physical access as required by CIP-004-1 R3. In addition, URE did not maintain documentation that URE conducted such training annually including the date the four employees completed the training and their attendance records. As a result, WECC Enforcement determined that URE failed to maintain documentation that URE conducted cyber security training at least annually, including the date the training was completed and attendance records as required by CIP-004-1 R2.3.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the CIP-004-1 R3 violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) but did pose a moderate risk. In this case, for about three months, approximately 9 percent of URE's personnel or contractors had access to CCAs without having a completed PRA. Without properly vetting the identity and criminal history of personnel, it was possible a person or persons with a negative background or criminal history could have accessed URE's assets essential to the operation of the BPS. Nonetheless, URE did have additional security measures (*e.g.*, a Corporate Security department and an Information Technology service) in place helping to mitigate a potential security threat. For these reasons, WECC determined this violation posed a moderate risk to the reliability of the BPS.

WECC determined that the CIP-004-1 R2 violation did not pose a serious or substantial risk to the reliability of the BPS because in this instance, URE's violation is limited to four personnel with physical access to CCAs out of its personnel with access to CCAs. Further, the four employees associated with this violation were long-time URE employees, had received initial training and URE had additional security measures (*e.g.*, Corporate Security department and an Information Technology service) in place helping to mitigate a potential security threat. For these reasons, WECC determined this violation posed minimal risk to the reliability of the BPS.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S)
R3: 7/1/09 (when the Standard became mandatory and enforceable for URE) through 3/19/10 (Mitigation Plan completion)
R2: 12/30/09 (when annual training was missed) through April 30, 2010 (Mitigation Plan completion)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY
R3: Self-Report
R2: 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.	**R3: MIT-09-2886 R2: MIT-09-3121**
DATE SUBMITTED TO REGIONAL ENTITY	**R3: 3/15/10 R2: 11/1/10**
DATE ACCEPTED BY REGIONAL ENTITY	**R3: 9/3/10 R2: 11/11/10**
DATE APPROVED BY NERC	**R3: 10/8/10 R2: 12/13/10**
DATE PROVIDED TO FERC	**R3: 10/8/10 R2: 12/14/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **R3: 3/31/10 R2: Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **R3: 3/19/10 R2: 4/30/2010**

DATE OF CERTIFICATION LETTER **R3: 4/1/10 R2:11/1/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **R3: 3/23/10 R2: 4/30/2010**

DATE OF VERIFICATION LETTER **R3: 9/24/10 R2: 6/21/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **R3: 3/19/10**[6]
R2: 4/30/2010

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

To mitigate CIP-004-1 R3, URE stated that (1) cyber and physical access requests now go through a multi-step review and approval process (Supervisor/Manager/Director) to ensure all requests have been reviewed and approved by management before programming is applied; (2) Corporate Security department performed database purges terminating physical access for individuals without background and training completions and provided the list to Information Technology service; (3) Corporate Security department and an Information Technology service updated and revised process documentation to ensure consistency and awareness of the procedural steps that must be followed for access programming completion; and (4) Corporate Security department developed a single database source for employees and contractors that will be used by Corporate Security department and an Information Technology service as verification of background and training requirement completions prior to access programming applied.

To mitigate CIP-004-1 R2, URE stated that it (1) will use the combined Corporate Security department database for all future training and background check updates; (2) prepared its cyber and physical access process maps to help identify control gaps and mitigated them; (3) revised its cyber and physical access procedures with process change details; and (4) notified and trained appropriate personnel regarding the changes.

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)

To demonstrate completion of the Mitigation Plan for CIP-004-1 R3, WECC reviewed the following documents: URE's procedure documents; training records; and evidence that URE completed a PRA for the employees in scope.

To demonstrate completion of the Mitigation Plan for CIP-004-1 R2, WECC reviewed the following documents: URE's Access database deletions;

[6] After reviewing the evidence WECC determined that URE was compliant with the CIP-004-1 R2 violation.

procedure documents; training agenda and sign-in sheets; SQL source database screen shot and field descriptions; and a flow chart

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-004-1 R3
URE's Self-Report for CIP-004-1 R2

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2886 for CIP-004-1 R3
URE's Mitigation Plan MIT-09-3121 for CIP-004-1 R2

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-004-1 R3
URE's Certification of Mitigation Plan Completion for CIP-004-1 R2

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion for CIP-004-1 R3
WECC's Verification of Mitigation Plan Completion for CIP-004-1 R2

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-005-1 R2 and R3

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment b-2

DISPOSITION OF VIOLATION

Dated May 9, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002082	**WECC2010-609979**
WECC201002088	**WECC2010-609980**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-005-1	**2**		**Medium**[1]	**Severe**[2]
CIP-005-1	**3**		**Medium**	**Severe**[3]

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

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

CIP-005-1 R2 provides:

> **R2. Electronic Access Controls — The Responsible Entity[4] shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).**
>
> > **R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.**

[1] CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" VRF; R2.5 and its sub-requirements and R2.6 each have a "Lower" VRF.
[2] WECC assessed a "Severe" VSL because URE did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
[3] WECC assessed a "Severe" VSL because URE did not implement electronic or manual processes monitoring and logging at 15% or more of its access points.
[4] Within the text of Standard CIP-005, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

CIP-005-1 R3 provides:

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

> **R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.**

(Footnote added.)

VIOLATION DESCRIPTION

WECC notified URE that WECC was initiating the semiannual CIP Self-Certification process. URE submitted a Self-Report addressing its noncompliance with CIP-005-1 R2 and R3 and approximately a week later, URE submitted its Self-Certification. Although URE self-reported these violations, because URE self-reported during the Self-Certification submission period, the discovery method for these violations is classified as Self-Certification.

URE stated in the Self-Report that it had determined that the documented method for remote access into an Electronic Security Perimeter (ESP) had not been used in all business applications and that some URE personnel used Virtual Private Network (VPN) and Remote Desktop Protocol (RDP) in violation of CIP-005-1 R2. The violation was the result of a legacy process being used by authorized users to access Critical Cyber Assets (CCAs) from outside the ESP. URE also stated that a system configuration error resulted in a failure to properly log user electronic access to ESPs in violation of CIP-005-1 R3. Furthermore, URE's link between the remote access server and the centralized log collection server was not functioning correctly, which was corrected upon discovery.

A WECC subject matter expert (SME) reviewed the URE's documentation and conducted a phone interview with a URE Manager. During the phone interview, the Manager confirmed that an unknown number of personnel used undocumented methods (*e.g.*, RDP and VPN) for accessing an unknown number of CCAs, but that the personnel in scope belonged to the URE protection group. The Manager stated that the ports and services used by the personnel (*e.g.*, RDP and VPN) should have been disabled. Accordingly, the SME determined URE did not implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESP, resulting in a violation of CIP-005-1 R2.

During the phone interview, the Manager also stated that during an internal review, URE discovered that access logs from certain devices were not being monitored and reviewed. The communication link between the central log server, where logs were

gathered from the devices, and the monitoring server broke. The SME determined these devices are part of URE's data network. Accordingly, the SME determined URE did not implement an electronic or manual process for monitoring and logging access at access points to the ESP twenty-four hours a day, seven days a week, resulting in a violation of CIP-005-1 R3.

The SME forwarded its findings to WECC Enforcement and WECC Enforcement determined URE personnel used undocumented mechanisms to access an unknown number of URE's CCAs. Specifically, URE failed to implement organizational processes and technical and procedural mechanisms for control of electronic access at all of URE's electronic access points to its ESPs as required by CIP-005-1 R2.

WECC Enforcement also determined that URE did not monitor personnel access to URE's ESP. Specifically, after URE's system configuration error, the link between URE's remote access server and the centralized collection server broke. In this case, URE failed to implement an electronic or manual process for monitoring and logging access at access points to the ESP twenty-four hours a day, seven days a week as required by CIP-005-1 R3.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the CIP-005-1 R2 violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) but did pose a moderate risk. Failure to document and implement mechanisms for control of electronic access to the ESP could have potentially exposed URE's CCAs within its ESP to security attacks. This increased exposure, from enabling ports and services not required for operations and monitoring Cyber Assets within the ESP, could have allowed for unauthorized internal or external access, which could have allowed for successful cyber attacks against CCAs essential for operation of the BPS. Nonetheless, URE did have additional security measures in place (*e.g.*, multiple log-in screens) helping to mitigate a potential security threat. In addition, the personnel in scope belonged to the URE protection group which had their personnel risk assessments done prior to accessing the CCAs. For these reasons, WECC determined this violation posed a moderate risk to the reliability of the BPS.

WECC determined that the CIP-005-1 R3 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 detect and alert unauthorized access at all access points to the ESP could have exposed CCAs within the ESP to malicious access attempts. This exposure could have compromised the security of the CCAs essential for the operation of the BPS. Nonetheless, URE did have additional security measures in place (*e.g.*, multiple log-in screens) helping to mitigate a potential security threat. In addition, the personnel in scope belonged to the URE protection group which had their personnel risk assessments done prior to accessing the CCAs. For these reasons, WECC determined this violation posed a moderate risk to the reliability of the BPS.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S)
R2: 7/1/09 (when the Standard became mandatory and enforceable for URE) through 3/23/10 (Mitigation Plan completion)
R3: 7/1/09 (when the Standard became mandatory and enforceable for URE) through 4/30/10 (Mitigation Plan completion)

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	☒

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**R2: MIT-09-2894 R3: MIT-09-2895**
DATE SUBMITTED TO REGIONAL ENTITY	**R2: 3/15/10 R3: 3/15/10**
DATE ACCEPTED BY REGIONAL ENTITY	**R2: 9/22/10 R3: 9/16/10**
DATE APPROVED BY NERC	**R2: 10/11/10 R3: 10/11/10**
DATE PROVIDED TO FERC	**R2: 10/13/10 R3: 10/13/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**R2: 4/1/10 R3: 5/1/10**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**R2: 3/23/10 R3: 4/30/10**
DATE OF CERTIFICATION LETTER	**R2: 4/1/10 R3: 5/3/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**R2: 3/31/10 R3: 4/30/10**
DATE OF VERIFICATION LETTER	**R2: 9/30/10 R3: 9/30/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**R2: 3/23/10**[5] **R3: 4/30/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

To mitigate CIP-005-1 R2, URE stated that it (1) obtained proper access for two authorized users that were using URE's legacy process; (2) submitted a firewall change request to allow RDP access to the ESPs and made changes to the firewall in accordance with URE's established change management process; and (3) disabled RDP access from the perimeter network through its secure data network zone.

To mitigate CIP-005-1 R3, URE stated that it (1) updated the three appliances so the "syslogs" are being sent to the centralized log server; (2) verified that "syslogs" reach the centralized log server; (3) updated back-up files for the appliances configuration document; (4) updated the appliances configuration document with the correct configuration for sending "syslogs" to the centralized log server; and (5) validated and documented the process for reporting log variances for CCAs that describes how the event log manager is used and managed within URE.

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)

To demonstrate completion of the Mitigation Plan for CIP-005-1 R2, WECC reviewed the following documents: URE's firewall exception request; an access validation document; and evidence of a remote access request.

To demonstrate completion of the Mitigation Plan for CIP-005-1 R3, WECC reviewed the following documents: URE's log verification; log manual; configuration and logging document; manual for server security; access configuration data, log data and e-mails.

[5] After reviewing the evidence WECC determined that URE mitigated the CIP-005-1 R2 violation.

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Certification

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2894 for CIP-005-1 R2
URE's Mitigation Plan MIT-09-2895 for CIP-005-1 R3

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-005-1 R2
URE's Certification of Mitigation Plan Completion for CIP-005-1 R3

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion for CIP-005-1 R2
WECC's Verification of Mitigation Plan Completion for CIP-005-1 R3

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007-1 R2 and R8

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

DISPOSITION OF VIOLATION
Dated May 9, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002080	**WECC2010-609981**
WECC200902081	**WECC2010-609983**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	**2**		**Medium**	**Severe**
CIP-007-1	**8**	**8.2**	**Medium**[1]	**Severe**[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…."

CIP-007-1 R2 provides:

> **R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.**
>
> > **R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.**
> >
> > **R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to**

[1] CIP-007-1 R8 and R8.1 each have a "Lower" VRF; R8.2, R8.3 and R8.4 each have a "Medium" VRF. In the context of this case, WECC determined the violation related to R8.2, and therefore a "Medium" VRF is appropriate.
[2] WECC assessed the "Severe" VSL based on the VSL Matrix for R8; there is no VSL provided for sub-requirement R8.2.
[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.

> **production use of all Cyber Assets inside the Electronic Security Perimeter(s).**
>
> **R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.**

CIP-007-1 R8 provides in pertinent part:

> **R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:**
>
> **…**
>
> **R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;**

(Footnote added.)

VIOLATION DESCRIPTION

CIP-007-1 R2

WECC notified URE that WECC was initiating the semiannual CIP Self-Certification process. URE submitted a Self-Report addressing its noncompliance with CIP-007-1 R2 and approximately a week later, URE submitted its Self-Certification. Although URE self-reported the violation, because URE self-reported during the Self-Certification submission period, the discovery method for this violation is classified as Self-Certification.

URE stated that a comprehensive review of required ports and services necessary for normal and emergency operations had not been adequately performed in violation of CIP-007-1 R2. URE also stated that the required configurations did not appear to be fully documented, but that it believed that no unauthorized ports or services were open.

A WECC subject matter expert (SME) reviewed URE's documentation and conducted a phone interview with a URE Manager. During the phone interview, the Manager stated URE's IT group began conducting port scans to determine the ports that should be enabled and disabled, that URE documented this process, but there was no baseline scan conducted and documented. As a result, URE was unaware of which ports and services should be enabled and was unable to verify and compare the subsequent scans to a baseline scan. The SME determined URE had been

scanning and reviewing its non-Windows-based systems. Thus, only Windows-based devices were associated with URE's reported violation. Based on the interview data request, the SME determined URE had approximately 400 devices used across a variety of functions, including Supervisory Control and Data Acquisition (SCADA), Human-Machine-Interface and Energy Management System (EMS). Accordingly, the SME determined URE did not establish and document a process to ensure that only those ports and services required for normal and emergency operations were enabled, resulting in a violation of CIP-007-1 R2.

The SME forwarded its findings to WECC Enforcement and WECC Enforcement determined that for these systems, because URE did not test its baselines for ports and services, it could not establish and document a process to ensure that only those ports and services required for normal and emergency operations were enabled as required by CIP-007-1 R2.

CIP-007-1 R8

URE discovered a violation of CIP-007-1 R8 during an internal review and submitted a Self-Report to WECC. According to the Self-Report, a comprehensive cyber vulnerability review had not been adequately performed or documented to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter (ESP) were enabled. This lack of assessment was in violation of CIP-007-1 R8.2. URE further stated that it did not have sufficient documentation in the form of configuration manuals or drawings that could be used to perform this review, but that it believed that no unauthorized ports or services were open.

A WECC subject matter expert (SME) reviewed URE's documentation and conducted a phone interview with a URE Manager. During the phone interview to determine compliance for R2 detailed above, the Manager stated URE's IT group began conducting port scans to determine the ports that should be enabled and disabled, that URE documented this process, but there was no baseline scan conducted and documented. As a result, URE was unaware of which ports and services should be enabled and was unable to verify and compare the subsequent scans to a baseline scan. Accordingly, the SME determined that URE did not conduct a review to verify that only ports and services required for operation of the Cyber Assets within URE's ESP were enabled, resulting in a violation of CIP-007-1 R8.2.

WECC Enforcement determined that for these systems, URE did not create a baseline for ports and services and failed to review its ports and services to ensure that only such ports and services required for operation of URE's Cyber Assets within its ESP were enabled. Specifically, URE failed to conduct a cyber vulnerability assessment that included such a review as required by CIP-007-1 R8.2.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the CIP-007-1 R2 and R8 violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because URE did have security measures (*e.g.*, routine vulnerability scans and documentation of monitoring logs) in place to mitigate a potential security threat. URE's lack of a process to establish a baseline and ensure that only those ports and services required for normal and emergency operations were enabled could have allowed for unauthorized internal and or external access to URE's Critical Cyber Assets (CCAs). This potential represented a moderate risk to the BPS.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT	**R8:** ☒
SELF-CERTIFICATION	**R2:** ☒
COMPLIANCE AUDIT	☐
COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK	☐
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

DURATION DATE(S)
7/1/09 (when the Standard became mandatory and enforceable for URE) through 12/15/10 (Mitigation Plan completion)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY
R2: Self-Certification
R8: 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	☒

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2868**
DATE SUBMITTED TO REGIONAL ENTITY	**3/15/10**
DATE ACCEPTED BY REGIONAL ENTITY	**9/14/10**
DATE APPROVED BY NERC	**10/7/10**
DATE PROVIDED TO FERC	**10/7/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **12/15/10**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **12/15/10**

DATE OF CERTIFICATION LETTER	**12/15/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**12/15/10**
DATE OF VERIFICATION LETTER	**3/11/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**12/15/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

To mitigate CIP-007-1 R2 and R8, URE stated that it (1) identified methods to discover ports and services and utilized this method to capture data and choose framework to ensure future compliance; (2) ensured that identified ports and services are mapped to devices; (3) documented requirements and updated the compliance tool; and (4) performed a ports and services review and followed the established remediation process.

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

To demonstrate completion of the Mitigation Plan, WECC reviewed the following documents:

(1) URE's lists of ports and services required for its systems and/or applications. The required ports and services lists were added to the existing configuration manuals/documentation for each asset group.

(2) URE's scan results and analysis of identified active ports and services not required for normal and emergency operations for the various applications and asset types. These scan results were compared with the lists and included in its process document, its stakeholder alert process manual and additional tracking documents.
(3) A document that outlined compliance requirements for CIP-007, including R2 (CCA Ports and Services) and R8 (CCA Annual Vulnerability Assessment).
(4) A document that described requirements (and tasks required) for managing ports and services in accordance with CIP-007 R2 (Ports and Services) and R8 (Annual Assessment to Review and Verify).
(5) URE's document routing requests were provided as evidence of approval and integration into existing process manuals and/or formalized stand-alone documents.

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Certification for CIP-007-1 R2
URE's Self-Report for CIP-007-1 R8

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2868 for CIP-007-1 R2 and CIP-007-1 R8

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-007-1 R2 and CIP-007-1 R8

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion for CIP-007-1 R2 and CIP-007-1 R8