PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

October 7, 2010

Ms. Kimberly Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 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 an Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Settlement Agreement and the Disposition Document, 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]

During a spot check, SERC Reliability Corporation (SERC) identified violations of: (1) CIP-002-1 R3 for URE's failure to include a time/frequency device located in its Control Center on its list of Critical Cyber Assets; (2) CIP-004-1 R2.1 for URE's failure to provide applicable cyber security training within ninety (90) days of granting fifteen (15) employees access to Critical Cyber Assets; and (3) CIP-004-1 R3 for URE's failure to conduct personnel risk assessments on forty-seven (47) contract employees within the required timeframe. This Notice of Penalty is being filed with the Commission because SERC and URE have entered into a

[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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Settlement Agreement to resolve all outstanding issues arising from a preliminary and non-public assessment resulting in SERC's determination and findings of the enforceable violations of CIP-002-1 R3, CIP-004-1 R2.1 and CIP-004-1 R3. According to the Settlement Agreement, URE admits that the facts set forth and agreed to by the parties for purposes of the Agreement constitute violations of NERC Reliability Standards CIP-002-1 R3 and CIP-004-1 R2.1 and R3, and has agreed to the proposed penalty of six thousand dollars ($6,000) to be assessed to URE, in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers SERC200900287, SERC200900288 and SERC200900289 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on December 17, 2009, by and between SERC and URE, which is included as Attachment d. The details of the findings and the basis for the penalty are set forth in the Disposition Documents included as Attachment e. This Notice of Penalty 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.

Region	NERC Violation ID	Reliability Std.[3]	Req. (R)	VRF	Total Penalty ($)
SERC	SERC200900287	CIP-002-1	3	High[4]	6,000
	SERC200900288	CIP-004-1	2.1	Medium[5]	

[3] CIP-002-1 through CIP-009-1 Standards were approved by the Commission on January 18, 2008 and have a mandatory implementation date of July 1, 2008 for registered entities with Balancing Authority and Transmission Operator functions.

[4] The Settlement Agreement, page 3 lists a "Medium" Violation Risk Factor (VRF) for CIP-002-1 R3. CIP-002-1 R3 was originally assigned a "Medium" VRF, which was in effect at the start of the violation. The Commission approved the VRF as filed, but directed NERC to submit a modification. On January 27, 2009, the Commission approved the modified "High" VRF. Therefore, the "Medium" VRF was in effect from June 18, 2007 through January 27, 2009 when the "High" VRF became effective. CIP-002-1 R3.1, R3.2 and R3.3 each have a "Lower" VRF.

[5] CIP-004-1 R2 has a "Lower" VRF and R2.1 had a "Lower" VRF which was in effect at the start of the violation. CIP-004-1 R2.1, R2.2 and R2.2.4 were originally assigned a "Lower" VRF. The Commission approved the VRFs as filed, but directed NERC to submit modifications. On January 27, 2009, the Commission approved the modified "Medium" VRFs. Therefore, the "Lower" VRFs were in effect from June 18, 2007 through January 27, 2009 when the "Medium" VRFs became effective. CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" VRF. CIP-004-1,R2.1 and R2.2 each have a "Medium" VRF effective January 27, 2009. CIP-004-1, R2.2.4 has a "Medium" VRF.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

	SERC200900289	CIP-004-1	3	Medium[6]	

The text of the Reliability Standards at issue is set forth in the Disposition Documents.

CIP-002-1 R3 - OVERVIEW[7]
SERC determined that URE, as a Balancing Authority and Transmission Operator, did not include all of the devices defined in the subject Standard on its list of Critical Cyber Assets. Specifically, SERC determined that a time/frequency device located in its Control Center was not included on URE's original list of Critical Cyber Assets.

The duration of the CIP-002-1 R3 violation was from July 1, 2008, when the Standard became mandatory and enforceable, through December 15, 2008, the date URE completed its Mitigation Plan.

SERC concluded that this violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the equipment in question was inside a secure perimeter and URE conservatively treats all equipment inside a secure as a Critical Cyber Asset even though it was not on the list.

CIP-004-1 R2.1 - OVERVIEW[8]
SERC determined that URE, as a Balancing Authority and Transmission Operator, did not provide applicable cyber security training within ninety (90) days of granting several employees access to Critical Cyber Assets. Specifically, SERC found fifteen (15) instances in which individuals had not received the required training within ninety (90) days of having access to Critical Cyber Assets.

The duration of the CIP-004-1 R2.1 violation was from July 1, 2008, when the Standard became mandatory and enforceable, through April 29, 2009, the date URE completed training of the last person identified as needing cyber security training.[9]

SERC concluded that this violation did not pose a serious or substantial risk to the reliability of the BPS because all affected personnel were familiar with the cyber assets and had been allowed access for several months prior to the requirement to be trained according to the Standard.

[6] The Settlement Agreement, page 6 lists a "Lower" VRF for CIP-004-1 R3 which was in effect at the start of the violation. CIP-004-1 R3 was originally assigned a "Lower" VRF. The Commission approved the VRF as filed, but directed NERC to submit a modification. On January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF was in effect from June 18, 2007 through January 27, 2009 when the "Medium" VRF became effective. CIP-004-1 R3.1, R3.2 and R3.3 each have a "Lower" VRF. CIP-004-1 R3 has a "Medium" VRF, effective January 27, 2009.
[7] Further information on this violation is contained in the Disposition Documents included as Attachment e to the Notice of Penalty.
[8] *Id.*
[9] The Mitigation Plan incorrectly states that the violation was mitigated on December 31, 2008.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

CIP-004-1 R3 - OVERVIEW[10]
SERC determined that URE, as a Balancing Authority and Transmission Operator, did not conduct personnel risk assessments on forty-seven (47) contract employees within the thirty (30) days when they were granted access as required by the subject Standard.

The duration of the CIP-004-1 R3 violation was from July 1, 2008, when the Standard became mandatory and enforceable, through October 29, 2008, the date URE completed the last required Personnel Risk Assessment.[11]

SERC concluded that this violation did not pose a serious or substantial risk to the reliability of the BPS because of the forty-seven (47) contractors for whom personnel risk assessments (PRAs) had not been conducted, only seven (7) had cyber access to Critical Cyber Assets. Further, the referenced contractors could only gain such cyber access from within the physical security perimeter, which was manned twenty-four hours/seven days a week by URE system supervisors for whom PRAs had been conducted prior to July 1, 2008 (the enforceable date). All of these contractors were well known to URE, having provided support services to URE for many years. All of URE's physical security perimeters are protected with access control systems and have been since well prior to July 1, 2008 and well prior to the time access was granted to the contractors. The badge reader system was monitored and logged such that URE could identify when individuals entered the secure areas. URE's electronic security perimeter (ESP) was secured with firewalls, with no remote access allowed, and the ESP was continuously monitored.

Regional Entity's Basis for Penalty
According to the Settlement Agreement, SERC has assessed a penalty of six thousand dollars ($6,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. the violations constituted URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE was cooperative throughout the compliance enforcement process;
3. URE has a compliance program, as discussed in the Disposition Documents;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations did not pose a serious or substantial risk to the BPS, as discussed above and in the Disposition Documents; and
6. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[10] *Id.*
[11] The Mitigation Plan incorrectly states that the violation was mitigated on November 1, 2008.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of six thousand dollars ($6,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Proposed Penalty, Sanction or Enforcement Action Imposed[12]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines, the Commission's July 3, 2008 and October 26, 2009 Guidance Orders,[13] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on May 14, 2010. The NERC BOTCC approved the Settlement Agreement, including SERC's imposition of a financial penalty, assessing a penalty of six thousand dollars ($6,000) 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 violations of the subject NERC Reliability Standards;
2. SERC reported that URE was cooperative throughout the compliance enforcement process;
3. URE has a compliance program, as discussed in the Disposition Documents;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations did not pose a serious or substantial risk to the BPS, as discussed above and in the Disposition Document; and
6. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approves the Settlement Agreement and believes that the assessed penalty of six thousand dollars ($6,000) is appropriate for the violation 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 Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

---

[12] *See* 18 C.F.R § 39.7(d)(4).

[13] *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). *See also North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Request for Confidential Treatment

Information in and certain attachments to the instant Notice of Penalty include privileged and 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. Specifically, this includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business and confidential information exempt from the mandatory public disclosure requirements of the Freedom of Information Act, 5 U.S.C. 552, and should be withheld from public disclosure.

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.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachments to be included as Part of this Notice of Penalty
The attachments to be included as part of this Notice of Penalty is the following documents and material:

a) SERC Audit Worksheet for CIP-002-1 R3 dated July 5, 2009, included as Attachment a;

b) SERC Audit Worksheet for CIP-004-1 R2.1 dated July 5, 2009, included as Attachment b;

c) SERC Audit Worksheet for CIP-004-1 R3 dated July 5, 2009, included as Attachment c;

d) Settlement Agreement by and between SERC and URE executed December 17, 2009, included as Attachment d;

   i. Record documents for the violation of CIP-002-1 R3:

      i. URE's Mitigation Plan dated September 2, 2009, included as Appendix A-1 to the Settlement Agreement;

      ii. URE's Certification of Completion dated October 14, 2009, included as Appendix A-2 to the Settlement Agreement; and

      iii. SERC's Verification of Completion dated November 2, 2009, included as Appendix A-3 to the Settlement Agreement.

   ii. Record documents for the violation of CIP-004-1 R2.1:

      i. URE's Mitigation Plan dated September 2, 2009, included as Appendix A-4 to the Settlement Agreement;

      ii. URE's Certification of Completion dated October 14, 2009, included as Appendix A-5 to the Settlement Agreement; and

      iii. SERC's Verification of Completion dated November 2, 2009, included as Appendix A-6 to the Settlement Agreement.

   iii. Record documents for the violation of CIP-004-1 R3, included as Attachment e:

      i. URE's Mitigation Plan dated September 2, 2009, included as Appendix A-7 to the Settlement Agreement;

      ii. URE's Certification of Completion dated October 14, 2009, included as Appendix A-8 to the Settlement Agreement; and

      iii. SERC's Verification of Completion dated November 2, 2009, included as Appendix A-9 to the Settlement Agreement.

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

   i. Disposition Document for CIP-002-1, included as Attachment e-1; and

   ii. Disposition Document for CIP-004-1, included as Attachment e-2.

A Form of Notice Suitable for Publication[14]
A copy of a notice suitable for publication is included in Attachment f.

[14] *See* 18 C.F.R § 39.7(d)(6).

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Notices and Communications

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

Gerald W. Cauley* President and Chief Executive Officer David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile gerry.cauley@nerc.net david.cook@nerc.net	Rebecca J. Michael* Assistant General Counsel Davis Smith* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net davis.smith@nerc.net
Kenneth B. Keels, Jr.* Director of Compliance Andrea Koch* Manager of Compliance Enforcement and Mitigation SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8214 (704) 357-7914 – facsimile kkeels@serc1.org akoch@serc1.org	R. Scott Henry* President and Chief Executive Officer SERC Reliability Corporation 2815 Coliseum Centre Drive Charlotte, NC 28217 (704) 940-8202 (704) 357-7914 – facsimile shenry@serc1.org Marisa A. Sifontes* General Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7775 (704) 357-7914 – facsimile msifontes@serc1.org Jacqueline E. Carmody* Legal Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7778 (704) 357-7914 – facsimile jcarmody@serc1.org
*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

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

Respectfully submitted,

/s/ *Rebecca J. Michael*

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

Rebecca J. Michael
Assistant General Counsel
Davis Smith
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
davis.smith@nerc.net

cc: Unidentified Registered Entity
SERC Reliability Corporation

Attachments

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment e

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

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

REGIONAL ENTITY
SERC Reliability Corporation (SERC)

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 PROPOSED PENALTY OR SANCTION, REGISTERED ENTITY

ACCEPTS IT/ DOES NOT CONTEST IT	YES	☒

I. PENALTY INFORMATION

TOTAL PROPOSED PENALTY OR SANCTION OF **$6,000** FOR **THREE** VIOLATIONS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST ANY CONFIRMED OR SETTLED 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.

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

LIST ANY PRIOR CONFIRMED OR SETTLED 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[2]
YES ☒ NO ☐
EXPLAIN

URE's compliance program was established in 2004 and encompasses more than just the NERC Reliability Standards. It addresses all regulatory compliance obligations for the company. URE has issued company policy which establishes the mandate to operate in a safe, legal, and efficient manner. This is achieved through good management practices which includes adherence to approved procedures used by well trained personnel coupled with strict compliance with applicable codes, standards, and regulations. This URE policy is supported with administrative and departmental programs and procedures necessary to achieve the policy directive.

DOES SENIOR MANAGEMENT TAKE ACTIONS THAT SUPPORT THE COMPLIANCE PROGRAM, SUCH AS TRAINING, COMPLIANCE AS A FACTOR IN EMPLOYEE EVALUATIONS, OR OTHERWISE
YES ☒ NO ☐
EXPLAIN

[2] SERC considered the existence of URE's Internal Compliance Program as a neutral factor in its penalty determination.

EXPLAIN SENIOR MANAGEMENT'S ROLE AND INVOLVEMENT WITH RESPECT TO THE REGISTERED ENTITY'S COMPLIANCE PROGRAM

URE's President is also its Chief Compliance Officer. He reports directly to the Board of Directors of the company. Other senior managers are directly responsible for implementing the policies, procedures and programs. URE also has in place in a Committee that is comprised of senior management. The Committee reviews and approves all the Administrative procedures and programs. URE senior management is very involved in its NERC Reliability Standard compliance efforts.

(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 (IF THE RESPONSE IS "YES," THE ABBREVIATED NOP FORM MAY NOT BE USED.)

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

(9) ADDITIONAL SUPPORT FOR PROPOSED PENALTY OR SANCTION

OTHER RELEVANT INFORMATION:

NOTICE OF ALLEGED VIOLATION AND PROPOSED PENALTY OR SANCTION ISSUED
DATE: OR N/A ☒

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **10/2/2009** 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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-002-1

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

DISPOSITION OF VIOLATION

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
SERC200900287	**09-046**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-002-1	**3**		**High**[1]	**Moderate**

VIOLATION APPLIES TO THE FOLLOWING FUNCTIONS:

BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	*TOP*	TP	TSP
X												*X*		

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

Purpose: Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the BPS. These Critical Assets are to be identified through the application of a risk-based assessment.

Requirement:
R3.

> **Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity[2] shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For**

[1] The Settlement Agreement, page 3 lists a "Medium" Violation Risk Factor (VRF) for CIP-002-1 R3. CIP-002-1 R3 was originally assigned a "Medium" VRF, which was in effect at the start of the violation. The Commission approved the VRF as filed, but directed NERC to submit a modification. On January 27, 2009, the Commission approved the modified "High" VRF. Therefore, the "Medium" VRF was in effect from June 18, 2007 through January 27, 2009 when the "High" VRF became effective. CIP-002-1 R3.1, R3.2 and R3.3 each have a "Lower" VRF.

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

the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

VIOLATION DESCRIPTION

During a spot check, SERC discovered a violation of CIP-002-1 R3 for Unidentified Registered Entity's (URE) failure to include a time/frequency device located in its Control Center on its list of Critical Assets. SERC determined that URE had created a list of Critical Cyber Assets as required by CIP-002-1 R3. URE's list of Critical Cyber Assets included its Control Center, but URE failed to consider all of the devices that met the definition for compliance with R3. Specifically, SERC found that a time/frequency device (time synchronization server) in the Control Center was inadvertently missed. However URE treats all equipment inside a secure perimeter as a Critical Cyber Asset, even though it was not included on URE's original list of associated Critical Cyber Assets.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

SERC Compliance Enforcement Staff concluded that there was no serious or substantial risk to the reliability of the BPS as a result this violation because the equipment in question was inside a secure perimeter and was a Critical Cyber Asset although it was not on the list.

III. 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)

7/1/2008 (the date the Standard was mandatory for URE) through 12/15/2008 (the date the time/frequency device was added to URE's list of Critical Cyber Assets)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **7/2/2009**

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 ☒

IV. MITIGATION INFORMATION

MITIGATION PLAN NO. **MIT-08-2006**[3]

DATE SUBMITTED TO REGIONAL ENTITY **9/2/2009**
DATE ACCEPTED BY REGIONAL ENTITY **9/24/2009**
DATE APPROVED BY NERC **9/28/2009**
DATE PROVIDED TO FERC **9/28/2009**

IDENTIFY AND EXPLAIN VERSIONS THAT WERE REJECTED, IF APPLICABLE

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **12/15/2008**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **12/15/2008**

DATE OF CERTIFICATION LETTER **10/14/2009**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **12/15/2008**

DATE OF VERIFICATION LETTER **11/2/2009**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **12/15/2008**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE added the time/frequency device (time synchronization server) to its list of Critical Cyber Assets. Further, URE has adopted a process that incorporates a review of URE's electronically generated inventory of components within the secured perimeter.

[3] The Mitigation Plan incorrectly identifies the Reliability Standard as CIP-002-1a.

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

1. **URE Critical Cyber Assets List;**
2. **URE Memorandum from Management to a URE regarding Identification Review for Time Synchronization Server; and**
3. **URE Memorandum from Management to a URE Computer Network Specialist regarding Server, Asset Information.**

EXHIBITS:

SOURCE DOCUMENT
SERC Audit Worksheet for CIP-002-1 R3 dated July 5, 2009

MITIGATION PLAN
URE's Mitigation Plan MIT-08-2006 for CIP-002-1 R3 submitted September 2, 2009

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Completion dated October 14, 2009

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-1

DISPOSITION OF VIOLATION

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
SERC200900288	**09-047**
SERC200900289	**09-048**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**2**	**2.1**	**Lower**[1] **Medium**	**Lower**
CIP-004-1	**3**		**Medium**[2]	**Moderate**

VIOLATION APPLIES TO THE FOLLOWING FUNCTIONS:

BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	*TOP*	TP	TSP
X												*X*		

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

Purpose: 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.

Requirements:
R2.

Training — The Responsible Entity[3] shall establish, maintain, and document an annual cyber security training program for personnel having authorized

[1] CIP-004-1 R2 has a "Lower" VRF and R2.1 had a "Lower" VRF which was in effect at the start of the violation. CIP-004-1 R2.1, R2.2 and R2.2.4 were originally assigned a "Lower" VRF. The Commission approved the VRFs as filed, but directed NERC to submit modifications. On January 27, 2009, the Commission approved the modified "Medium" VRFs. Therefore, the "Lower" VRFs were in effect from June 18, 2007 through January 27, 2009 when the "Medium" VRFs became effective. CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" VRF. CIP-004-1, R2.1 and R2.2 each have a "Medium" VRF effective January 27, 2009. CIP-004-1, R2.2.4 has a "Medium" VRF.

[2] The Settlement Agreement, page 6 lists a "Lower" VRF for CIP-004-1 R3 which was in effect at the start of the violation. CIP-004-1 R3 was originally assigned a "Lower" VRF. The Commission approved the VRF as filed, but directed NERC to submit a modification. On January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF was in effect from June 18, 2007 through January 27, 2009 when the "Medium" VRF became effective. CIP-004-1 R3.1, R3.2 and R3.3 each have a "Lower" VRF. CIP-004-1 R3 has a "Medium" VRF, effective January 27, 2009.

cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization…

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.

VIOLATION DESCRIPTION

During a spot check, SERC discovered violations of:

(1) CIP-004-1 R2.1 for Unidentified Registered Entity's (URE)URE failure to provide applicable cyber security training within ninety (90) days of granting fifteen (15) employees access to Critical Cyber Assets. URE provided a list to SERC of personnel that had received the required training. SERC selected nineteen (19) records for investigation and determined that in fifteen (15) of those cases, training had not been completed as required; and,
(2) CIP-004-1 R3 for URE's failure to have personnel risk assessments conducted on forty-seven (47) contract employees within thirty (30) days of

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

the contract employees being granted access. URE did not anticipate the difficulty in having all of its contractors provide the necessary personnel risk assessments. Consequently, URE sent a letter to its contractors informing them of the need to perform a Personnel Risk Assessment on each of their employees. Each contractor acted to perform the required assessments and reported the results to URE.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

With regard to CIP-004-1 R2.1, SERC concluded that there was no serious or substantial risk to the reliability of the bulk power system (BPS) as all affected personnel were familiar with and had access to the Cyber Assets for several months prior to the effective date of the Reliability Standard training requirement. Further, the seven (7) contractors with access to Critical Cyber Assets had established a consistent course of conduct and maintained a level of trust regarding the protection of URE's Critical Cyber Assets. URE's Critical Cyber Assets had not significantly changed between the effective date of the standard and the time when these contract employees received training,

With regard to CIP-004-1 R3, SERC concluded that this violation did not pose a serious or substantial risk to the reliability of the BPS because of the forty-seven (47) contractors with physical access for whom personnel risk assessments (PRAs) had not been conducted, only seven (7) had cyber access to Critical Cyber Assets and could only gain such cyber access from within the physical security perimeter which was manned 24x7 by URE system supervisors for whom PRAs had been conducted prior to July 1, 2008 (the enforceable date). All of these contractors were well known to URE having provided support services to URE for many years. All of URE's physical security perimeters are protected with access control systems and have been since well prior to July 1, 2008 and well prior to the time access was granted to the contractors. The badge reader system was monitored and logged such that URE could identify when individuals entered the secure areas. URE's electronic security perimeter was secured with firewalls, with no remote access allowed, and the ESP was continuously monitored.

III. 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)

R2.1:
7/1/2008 (the date the Standard was mandatory for URE) through 4/29/2009 (when training was completed)[4]

R3:
7/1/2008 (the date the Standard was mandatory for URE) through 10/29/2008 (when personnel risk assessments were completed)[5]

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **7/2/2009**

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 ☒

IV. MITIGATION INFORMATION

MITIGATION PLAN NO. **R2.1: MIT-09-2007**[6]
R3: MIT-09-2008[7]

R2.1 & R3:

DATE SUBMITTED TO REGIONAL ENTITY	**9/2/2009**
DATE ACCEPTED BY REGIONAL ENTITY	**9/24/2009**
DATE APPROVED BY NERC	**9/28/2009**
DATE PROVIDED TO FERC	**9/28/2009**

IDENTIFY AND EXPLAIN VERSIONS THAT WERE REJECTED, IF APPLICABLE

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**R2.1:**	**4/29/2009**
	R3:	**11/1/2008**
EXTENSIONS GRANTED	**N/A**	
ACTUAL COMPLETION DATE	**R2.1:**	**4/29/2009**[8]
	R3:	**10/29/2008**

[4] The Mitigation Plan incorrectly states that the violation was mitigated on December 31, 2008.
[5] The Mitigation Plan incorrectly states that the violation was mitigated on November 1, 2008.
[6] The Mitigation Plan incorrectly identifies the Standard as CIP-004-1a.
[7] *Id.*
[8] *See* n.4.

DATE OF CERTIFICATION LETTER(S): **R2 & R3: 10/14/2009**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF:
R2.1: 4/29/2009
R3: 10/29/2008

DATE OF VERIFICATION LETTER(S): **R2 & R3: 11/2/2009**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF:
R2.1: 4/29/2009
R3: 10/29/2008

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

R2.1:
URE trained all personnel with unescorted physical access to Critical Cyber Assets. New personnel requiring access to Critical Cyber Assets are permitted to do so after completing the required training. Additionally, URE changed its procedures controlling access to Critical Cyber Assets to require the training specified in CIP-004-1 to occur prior to receiving that access. The documentation of the training must be submitted to the site training group before the site security grants access privileges. URE's manager of security will conduct quarterly reviews of training records to determine which employees will require upcoming training.

R3:
Personnel Risk Assessments were completed for all contractors with unescorted physical access to Critical Cyber Assets. Additionally, URE changed the procedures that control access to its Critical Cyber Assets to require that completion of the background checks specified in NERC Reliability Standard CIP-004-1 occur prior to an individual receiving access to Critical Cyber Assets. Contractors needing access to areas containing Critical Cyber Assets must be escorted if a Personnel Risk Assessment has not been completed and unescorted access is not granted until a satisfactory Personnel Risk Assessment has been performed. The access privilege requirement is included in the contents of URE's Cyber Security Training.

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

SERC reviewed, in support of the mitigation of R2.1:

(1) URE's administrative program document that outlines the company's overall cyber security program and CIP compliance strategy;

(2) URE's Infrastructure Protection Procedure that identifies and establishes the processes for ensuring that personnel with unescorted physical or electronic access have been properly trained and assessed for risk; and

(3) Records of the performance of the required training and physical security records including evidence of personnel risk assessments.

SERC reviewed, in support of the mitigation of R3:

URE's Contractor Background Check Status Report.

EXHIBITS:

SOURCE DOCUMENT

SERC Audit Worksheet for CIP-004-1 R2.1 dated July 5, 2009

SERC Audit Worksheet for CIP-004-1 R3 dated July 5, 2009

MITIGATION PLAN

URE's Mitigation Plan MIT-08-2007 for CIP-004-1 R2.1 submitted September 2, 2009

URE's Mitigation Plan MIT-08-2008 for CIP-004-1 R3 submitted September 2, 2009

CERTIFICATION BY REGISTERED ENTITY

URE's Certification of Completion for CIP-004-1 R2.1 dated October 14, 2009
URE's Certification of Completion for CIP-004-1 R3 dated October 14, 2009