NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 30, 2011

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Document attached thereto, 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 SERC Reliability Corporation (SERC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of the violations of CIP-004-1 Requirement (R) 2/2.3 and R3. According to the Settlement Agreement, URE admits the violations and has agreed to the assessed penalty of seven thousand dollars ($7,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers SERC200900337 and SERC200900338 are being filed in accordance with 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 (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

Statement of Findings Underlying the Violations

This NOP incorporates the findings and justifications set forth in the Settlement Agreement executed on March 23, 2011, by and between SERC and URE. The details of the findings and the basis for the penalty are set forth in the Disposition Documents. This NOP filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7, NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
NOC-722	SERC200900337	CIP-004-1	2/2.3	Lower[3]	1/1/09-10/16/09	7,000
	SERC200900338	CIP-004-1	3	Lower[4]	7/1/08-10/16/09	

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

CIP-004-1 R2/2.3 - OVERVIEW

As a result of a spot check, SERC determined that URE did not maintain required annual cyber security training documentation, including the date the training was completed or attendance records for approximately 7.0% employees and vendors listed on URE's Critical Cyber Asset (CCA) access list.

CIP-004-1 R3 - OVERVIEW

As a result of the Spot Check, SERC determined that URE did not have documentation verifying that personnel risk assessments (PRAs) had been conducted within seven years for approximately 6.6% employees and vendors.

[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. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[4] CIP-004-1 R3 has a "Medium" Violation Risk Factor (VRF); R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-004-1 R3 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines, the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[6] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on February 15, 2010. The NERC BOTCC approved the Settlement Agreement, including SERC's assessment of a seven thousand dollar ($7,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. the violations constituted URE's first violation of the subject NERC Reliability Standard;
2. SERC reported that URE was cooperative throughout the compliance enforcement process;
3. URE had an internal compliance program at the time of the violations which SERC considered a mitigating factor, as discussed in the Disposition Document;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. SERC determined that the violations 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 Document; and
6. SERC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement. The NERC BOTCC believes that the assessed penalty of seven thousand dollars ($7,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

---

[5] *See* 18 C.F.R. § 39.7(d)(4).

[6] *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).

Request for Confidential Treatment

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

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

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

Attachments to be included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between SERC and URE executed March 23, 2011, included as Attachment a;

    i. Disposition Document and SERC's Verification of Mitigation Plan Completion contained therein for CIP-004-1 R2 and R3, included as an attachment to the Settlement Agreement;

b) SERC's Screening Worksheet for URE's violation of CIP-004-1 R2/2.3, included as Attachment b;

c) SERC's Screening Worksheet for URE's violation of CIP-004-1 R3, included as Attachment c;

d) URE's Mitigation Plan for CIP-004-1 R2/2.3 submitted March 1, 2010, included as Attachment d;

e) URE's Mitigation Plan for CIP-004-1 R3 submitted March 1, 2010, included as Attachment e;

f) URE's Certification of Mitigation Plan Completion for CIP-004-1 R2/2.3 dated November 1, 2010, included as Attachment f; and

g) URE's Certification of Mitigation Plan Completion for CIP-004-1 R3 dated November 1, 2010, included as Attachment g.

A Form of Notice Suitable for Publication[7]

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

[7] *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 *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters 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 R. Scott Henry* President and CEO 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 Kenneth B. Keels, Jr.* Director of Compliance Andrea Koch* Manager, Compliance Enforcement and Mitigation SERC Reliability Corporation 2815 Coliseum Centre Drive Charlotte, NC 28217 (704) 940-8214 (704) 357-7914 – facsimile kkeels@serc1.org akoch@serc1.org

Conclusion

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

Respectfully submitted,

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

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

cc: Unidentified Registered Entity
SERC Reliability Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document and SERC's Verification of Mitigation Plan Completion contained therein for CIP-004-1 R2 and R3

DISPOSITION OF VIOLATION[1]

Dated March 23, 2011

NERC TRACKING NO.	SERC TRACKING NO.
SERC200900337	09-098
SERC200900338	09-099

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	NCRXXXXX	NOC-722

REGIONAL ENTITY
SERC Reliability Corporation (SERC)

I. VIOLATION INFORMATION

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

[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.

[2] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" Violation Risk Factor (VRF); R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[3] At the time of the violations, no VSLs were in effect for CIP-004-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications. On May 17, 2010, NERC submitted a compliance filing in response to the March 18, 2010 order, which FERC accepted on September 18, 2010. SERC Compliance Enforcement staff assessed a "Severe" VSL for the violation of CIP-004-1 R2.3 based on the March 3, 2010 VSL matrix filed with the Commission because URE did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records. SERC Compliance Enforcement staff assessed a "Moderate" VSL for the violation of the CIP-004-1 R3 based on the March 3, 2010 VSL matrix because URE did not update PRAs for each employee with access to CCAs at least every seven years after the initial PRAs were performed pursuant to CIP-004-1 R3.2. Additionally, URE did not document the results of its PRAs for 5% or

(continued)

CIP-004-1	**3**	**3.2, 3.3**	**Lower**[4]	**N/A**

**Violation Risk Factor ("VRF")*
***Violation Severity Level ("VSL")*

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

The purpose 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 and R3 provide in pertinent part:

> **R2.** Training — The Responsible Entity 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.
>
> …
>
> **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.
>
> **R3.** Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:
>
> …
>
> **R3.2.** The Responsible Entity shall update each personnel risk

more, but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to CCAs, pursuant to CIP-004-1 R3.3.

[4] CIP-004-1 R3 has a "Medium" Violation Risk Factor (VRF); R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-004-1 R3 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

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

URE has a system control center that was required to self-certify compliance to NERC's Urgent Action Cyber Security Standard 1200 (UA 1200) and is, therefore, a "Table 1 Entity" under the Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1. As such, URE was required to be "Compliant" with NERC Reliability Standard CIP-004-1 R2 and R3 as of July 1, 2008 and "Auditably Compliant" as of July 1, 2009.

CIP-004-1 R2.3 (09-098)

The SERC spot check team reviewed a sample of records regarding annual cyber security training of URE employees for calendar year 2008. URE reported to the SERC spot check team that it defined "annual," for purposes of conducting required cyber-security training, to be a calendar year. The SERC spot check team discovered six (6) employees listed on URE's Critical Cyber Asset (CCA) access list for whom documentation of required annual cyber security training for calendar year 2008 could not be produced. The SERC spot check team reported the finding to URE and to SERC Compliance Enforcement staff.

Upon receipt of the CIP spot check findings, SERC Compliance Enforcement staff began its assessment of the violation. SERC Compliance Enforcement staff reviewed the spot check findings, and records from an internal review of training records of all employees with authorized access to CCA areas conducted by URE after the CIP spot check. The records indicated that approximately 7.0% of the employees and vendors for whom records of annual cyber security training did not exist for the 2008 calendar year.

As a result of its assessment, SERC Compliance Enforcement staff determined that URE had a violation of CIP-004-1 R2.3 because it did not maintain documentation, including the date the training was completed or attendance records, that required cyber security training was conducted annually for approximately 7.0% of the employees and vendors listed on URE's CCA access list.

CIP-004-1 R3 (09-099)

During the CIP spot-check, the SERC spot check team reviewed a spreadsheet listing the dates for Personal Risk Assessments (PRA) for employees with access to URE's CCAs. The spot check team found that URE did not have documentation verifying current PRAs for 6 employees.

URE had performed a review in 2006 of PRAs conducted in 2002 for employees on the CCA access lists. The review was to verify that all documentation of a PRA existed for each employee with CCA access within the previous seven years. A spreadsheet was created and the review noted that the PRAs were completed in 2006.

Upon review of URE's spreadsheet, the SERC spot check team determined that, while the spreadsheet indicated dates for PRAs conducted since 2002, no documentation was available to support the dates. Since URE could not provide documentation of current PRAs performed, the SERC spot check team was unable to verify that all personnel received PRAs within 30 days of access to CCAs being granted and was also unable to document that the PRAs were performed every seven years. The SERC spot check team sampled URE's CCA access lists and found at least three personnel for whom URE could not provide documentation of PRAs in violation of CIP-004-1 R3.

Upon receipt of the CIP spot check findings, SERC Compliance Enforcement staff began its assessment of the violation. SERC Compliance Enforcement staff reviewed the spot check findings and records from an internal review conducted by URE of PRAs for all of its employees that had access to CCA areas. SERC Compliance Enforcement staff found that URE did not have documentation verifying that PRAs had been conducted within seven years for approximately 6.6% of the employees and vendors.

As a result of its assessment, SERC Compliance Enforcement staff finds that URE also had a violation of CIP-004-1 R3 because URE failed to provide documentation that PRAs had been performed for all personnel who have authorized cyber or authorized unescorted physical access to CCAs every seven years as specified in CIP-004-1 R3.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

SERC finds that the violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:

1. the approximately 7.0% of the employees and vendors who did not have records of completing training in 2008 were long term employees of URE and had attended the required annual cyber security training in 2007;

2. the approximately 6.6% of the employees and vendors for whom PRAs had not been conducted within the past seven years, all but one of URE's employees had previous PRAs documented in 2002; and
3. the one employee who did not have a documented 2002 PRA was a long-term employee, in good standing, hired in 1991, at which time a background check had been conducted.

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	☒

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)

CIP-004-1 R2.3 (09-098) - January 1, 2009, the first day following the calendar year after the July 1, 2008 mandatory and enforceable date of CIP-004-1 R2.3 for URE, when URE should have documented that annual cyber security training had been conducted for the calendar year 2008, until October 16, 2009, when URE completed and documented annual cyber security training for calendar year 2009 for all required personnel.

CIP-004-1 R3 (09-099) - July 1, 2008, when the Standard became mandatory and

enforceable for URE, to October 16, 2009, when URE verified PRA documentation for all required personnel.

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY
Spot Check

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

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

IV. MITIGATION INFORMATION

CIP-004-1 R2.3 (09-098)

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	MIT-08-2946
DATE SUBMITTED TO REGIONAL ENTITY	March 1, 2010
DATE ACCEPTED BY REGIONAL ENTITY	October 14, 2010
DATE APPROVED BY NERC	October 27, 2010
DATE PROVIDED TO FERC	October 27, 2010

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

N/A

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	Submitted as complete
EXTENSIONS GRANTED	None
ACTUAL COMPLETION DATE	February 1, 2010

DATE OF CERTIFICATION LETTER November 1, 2010
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF February 1, 2010

DATE OF VERIFICATION November 19, 2010[5]
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF February 1, 2010

CIP-004-1 R3 (09-099)

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	MIT-08-3002
DATE SUBMITTED TO REGIONAL ENTITY	March 1, 2010
DATE ACCEPTED BY REGIONAL ENTITY	October 19, 2010
DATE APPROVED BY NERC	November 16, 2010
DATE PROVIDED TO FERC	November 18, 2010

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

N/A

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	Submitted as complete
EXTENSIONS GRANTED	N/A
ACTUAL COMPLETION DATE	February 1, 2010

DATE OF CERTIFICATION LETTER November 1, 2010
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF February 1, 2010

DATE OF VERIFICATION November 19, 2010
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF February 1, 2010

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

To correct the violations of CIP-004-1 R2.3 and R3, URE completed the following actions detailed in its Mitigation Plans:

1. URE took immediate steps to remediate all potential violations of CIP-004-1 R2.3 and R3. Access was denied immediately upon discovery of a missing Cyber Security training document or an invalid PRA. Once the remediation was

[5] This Disposition Document serves as SERC's Verification of Mitigation Plan Completion.

complete, there was no reliability risk to the BPS;

2. Consolidated all access lists and created only one CCA access list that is now maintained by the URE by October 13, 2009;

3. Verified the CCA training and PRA for each person on the master CCA access list. If the CCA training or PRA documentation did not exist or was not in the form necessary to meet the requirements set forth in the standard, then that employee's access was revoked. This action was expected to be completed by October 16, 2009;

4. Created a procedure for granting access to CCA areas. The procedure requires the compliance department to review all requests to ensure a proper PRA is available and the CCA training has been completed and properly documented. This action was expected to be completed by February 1, 2010; and

5. At a minimum of once per quarter, staff in the compliance department reviews each CCA access list to ensure that no employee without current PRA and CCA training have access.

To prevent recurrence of another violation of CIP-004-1 R2.3 and R3, URE completed the following actions detailed in its Mitigation Plans:

1. URE improved its Centralized Records Management program:
    a. Personnel Risk Assessments (PRA) and Cyber Security training records were dispersed throughout two divisions within URE;
    b. The compliance department now has the authority to maintain records pertaining to CIP-004 and to view and maintain employee background data. This will reduce the likelihood of future ambiguity regarding storage and tracking of Cyber Security training and PRA records.
2. URE enhanced its resources:
    a. A central repository stores documentation and electronic copies of the PRA and Cyber Security training records, linked to each employee within the access list. This custom library contains history and timelines, and integrates both into URE's enhanced defined processes.
    b. A knowledge base is used to centrally document the compliance processes. Specifying a single document will reduce or eliminate the risk of tracking errors.

c. URE's board of directors has approved additional positions for the NERC compliance team in the compliance department. The additional staffing resources will assist in preventing transition issues over personnel changes which can result in possible violations.

3. URE has improved its communications in several ways.
   a. With the use of knowledge bases, compliance practice knowledge has been dispersed more effectively to all appropriate responsible groups. Formal job description changes will place compliance responsibilities on appropriate information services division employees. Improvements made to the training system permits increased opportunities for communication of security awareness. A new email distribution list allows for easier communication to those on the access list.
   b. URE uses document management software for the further refinement of existing access request validation and access change documentation processes. These well-defined processes provide more consistent application to meet compliance needs. Personnel responsible for performing these functions now partner with compliance staff and assist in maintaining the process definitions.

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

URE provided the following evidence of completion of its approved Mitigation Plans:

1. An attestation from URE's manager of compliance to SERC stating that:
   - Milestone 1 of the Mitigation Plan was completed October 13, 2009.
   - Milestone 2 of the Mitigation Plan was completed October 16, 2009.
   - Milestone 3 of the Mitigation Plan was completed on February 1, 2010.

2. URE's procedure to be implemented for any requests for access to URE's CCAs. The procedure requires training to have been provided within one year prior to access and a PRA to have been performed within 5 years prior to access being granted to URE's CCAs.

3. A spreadsheet dated November 18, 2009, listing individuals with access to URE's CCAs, their latest training dates and the date of last PRA. The

spreadsheet shows that all individuals with current access to CCAs are current with training requirements and PRAs as required by CIP-004-1 R2 and R3.

4. A sample training record for the individual on line #4 of the above spreadsheet, showing the detailed training record of the individual.

5. A sample PRA sheet from URE's document management system, dated November 18, 2010, for the individual on line #4 of the above spreadsheet, showing the background checks run and the date the check was completed.

6. URE's Cyber Security training program, revised March 31, 2010, showing that URE has defined "annual" as first day of the calendar year to seventh day of the subsequent calendar year.

7. An email which shows preparations to roll out the annual training for the 2010 calendar year.

8. A random representative sample of records of training and risk assessments for persons on the current (November 18, 2010) and earlier access list to verify that steps described in URE's procedure were performed.

V. PENALTY INFORMATION

TOTAL ASSESSED PENALTY OR SANCTION OF SEVEN THOUSAND DOLLARS FOR TWO VIOLATIONS OF RELIABILITY STANDARDS.

(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

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
YES ☒ NO ☐
EXPLAIN

SERC considered URE's Compliance Program to be 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

EXHIBITS:

SERC AUDIT SCREENING WORKSHEET FOR CIP-004-1 R2.3

SERC AUDIT SCREENING WORKSHEET FOR CIP-004-1 R3

URE MITIGATION PLAN FOR CIP-004-1 R2.3, submitted March 1, 2010

URE MITIGATION PLAN FOR CIP-004-1 R3, submitted March 1, 2010

URE CERTIFICATION OF COMPLETION OF MITIGATION PLAN FOR CIP-004-1 R2.3, dated November 1, 2010

URE CERTIFICATION OF COMPLETION OF MITIGATION PLAN FOR CIP-004-1 R3, dated November 1, 2010

OTHER RELEVANT INFORMATION:

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

SETTLEMENT DISCUSSIONS COMMENCED
DATE: March 19, 2010 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