PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

April 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 Settlement Agreement (Attachment a) and the Disposition Document attached thereto (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 Reliability*First* Corporation (Reliability*First*) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from Reliability*First*'s determination and findings of the violations of CIP-004-1 Requirement (R) 2.3 and R4.2 and CIP-006-1 R1.8. According to the Settlement Agreement, URE admits the violations and has agreed to the assessed penalty of fifteen thousand dollars ($15,000), 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.

[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

Accordingly, the violations identified as NERC Violation Tracking Identification Numbers RFC201000307, RFC201000308, and RFC200900232 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This NOP incorporates the findings and justifications set forth in the Settlement Agreement executed on January 13, 2011, by and between Reliability*First* 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-767	RFC201000307	CIP-004-1	2.3	Lower[3]	6/30/09-3/24/10	15,000
	RFC201000308	CIP-004-1	4.2	Lower[4]	7/1/08-3/1/11	
	RFC200900232	CIP-006-1	1.8	Lower[5]	8/12/09-11/3/10	

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 R2.3 and R4.2 - OVERVIEW

During a spot check conducted, Reliability*First* identified violations of CIP-004-1 R2.3 and R4.2. Reliability*First* determined that URE did not (1) provide documentation that a contractor with cyber access to Critical Cyber Assets completed annual cyber security training in 2009; and (2) revoke, within seven calendar days, access to Cyber Security Assets for 3 individuals who no longer required such access.

CIP-006-1 R1.8 - OVERVIEW

On December 20, 2009, URE self-reported a violation of CIP-006-1 R1.8. Reliability*First* determined that URE did not afford the protective measures specified in CIP-007-1 R1 to

[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.

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

[5] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; R1.7 and R1.8 each have a "Lower" VRF.

security patches installed on security guard workstations that URE designated as Cyber Security Assets.[6]

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[7]

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,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on March 11, 2011. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of a fifteen thousand dollar ($15,000) 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 Standards;
2. URE self-reported the CIP-006-1 violation;
3. Reliability*First* reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violations which Reliability*First* 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. Reliability*First* determined that the violations posed a moderate 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. Reliability*First* reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[6] URE also self-reported a violation of CIP-007-1 R1, which was dismissed on January 7, 2011 because CIP-007-1 R1 is not applicable to the security guard workstations at issue since they are not within the Electronic Security Perimeter. The dismissed violation of CIP-007-1 R1 is included in the Mitigation Plan and Certification of Completion for CIP-006-1 R1.8.

[7] *See* 18 C.F.R. § 39.7(d)(4).

[8] *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).

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of fifteen thousand dollars ($15,000) 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.

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 Reliability*First* and URE executed December 3, 2010, included as Attachment a;
    a. Reliability*First*'s Summary of Possible Violation for CIP-004-1 R2.3, included as Attachment A to the Settlement Agreement;
    b. Reliability*First*'s Summary of Possible Violation for CIP-004-1 R4.2 , included as Attachment B to the Settlement Agreement;
    c. URE's Self-Report for CIP-006-1 R1.8 dated December 20, 2009, included as Attachment C to the Settlement Agreement;
    d. URE's Mitigation Plan for CIP-004-1 R2.3 designated as MIT-10-3207 submitted November 10, 2010, included as Attachment D to the Settlement Agreement;
    e. URE's Certification of Mitigation Plan Completion for CIP-004-1 R2.3 dated November 10, 2010, included as Attachment E to the Settlement Agreement;
    f. URE's Mitigation Plan for CIP-004-1 R4.2 designated as MIT-09-3208 submitted November 10, 2010, included as Attachment F to the Settlement Agreement;
    g. URE's Mitigation Plan for CIP-006-1 R1.8 designated as MIT-09-3122 submitted November 10, 2010, included as Attachment G to the Settlement Agreement;
    h. URE's Certification of Mitigation Plan Completion for CIP-006-1 R1.8 dated November 10, 2010, included as Attachment H to the Settlement Agreement;
b. Disposition Document for Common Information, included as Attachment b;
    a. Disposition Document for CIP-004-1 R2.3 and R4.2, included as Attachment b-1;
    b. Disposition Document for CIP-006-1 R1.8, included as Attachment b-2;
c. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R2.3 dated April 25, 2011, included as Attachment c;
d. URE's Certification of Mitigation Plan Completion for CIP-004-1 R4.2 dated April 12, 2011, included as Attachment d;
e. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R4.2 dated April 25, 2011, included as Attachment e; and

f. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-1 R1.8 dated April 12, 2011, included as Attachment f.

A Form of Notice Suitable for Publication[9]

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

[9] *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 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 Robert K. Wargo* Director of Enforcement and Regulatory Affairs Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 bob.wargo@rfirst.org L. Jason Blake* Corporate Counsel Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 jason.blake@rfirst.org Michael D. Austin* Associate Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 mike.austin@rfirst.org Amanda E. Fried* Associate Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 amanda.fried@rfirst.org

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

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

Respectfully submitted,

/s/ *Rebecca J. Michael*

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

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

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment b

Disposition Document for Common Information

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS

Dated March 11, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-767**

REGIONAL ENTITY
Reliability*First* Corporation (Reliability*First*)

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 **$15,000** FOR **THREE** 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
N/A

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
Reliability*First* considered certain aspects of URE's internal compliance program (ICP) as mitigating factors.

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

Reliability*First* favorably considered that URE self reported one of these alleged violations but also considered that two of the violations were discovered at a Compliance Spot Check.

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

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

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **7/30/10** OR N/A ☐

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

SUPPLEMENTAL RECORD INFORMATION
DATE(S) OR N/A ☒
REGISTERED ENTITY RESPONSE CONTESTED
FINDINGS ☐ PENALTY ☐ BOTH ☐ DID NOT CONTEST ☒

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-1 R2.3 and R4.2

DISPOSITION OF VIOLATION
Dated March 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000307	**RFC201000307**
RFC201000308	**RFC201000308**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**2**	**2.3**	**Lower**[1]	**N/A**[2]
CIP-004-1	**4**	**4.2**	**Lower**[3]	**N/A**[4]

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-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."

CIP-004-1 R2 states, in pertinent part:

> **R2. Training — The Responsible Entity[5] shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.**
>
> *******

[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.
[2] VSLs were not in effect during the duration of the subject violation.
[3] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF. When NERC filed VRFs, it originally assigned CIP-004-1 R4.2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-004-1 R4.2 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.
[4] VSLs were not in effect during the duration of the subject violation.
[5] Within the text of Standard CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

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 R4 states:

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

VIOLATION DESCRIPTION

Reliability*First* conducted a Compliance Spot Check of URE. During the spot check, Reliability*First* identified a violation of CIP-004-1 R2.3 because URE did not maintain documentation indicating that cyber security training was conducted at least annually. According to the Settlement Agreement, a contractor with access to Critical Cyber Assets completed cyber security training in 2008, but did not complete cyber security training is 2009. URE granted the subject contractor cyber access to Cyber Security Assets on June 30, 2008 after the contractor completed cyber security training. URE notified the contractor of the need to complete annual training in 2009, but, due to technical issues with access to the on-line training material, the individual failed to complete the training by June 30, 2009 in accordance with the subject Standards requirement.[6]

During the spot check, Reliability*First* also identified a violation of CIP-004-1 R4.2 as URE failed, on three occasions, to revoke access to Cyber Security Assets within seven calendar days for personnel who no longer required such access. According to the Settlement Agreement, on October 3, 2008, an URE employee transferred positions and no longer required unescorted physical access. Although URE timely revoked the employee's cyber access, it did not revoke the individual's authorized unescorted physical access until October 15, 2008. On two other occasions, an URE employee and an URE contractor retired on June 4, 2009 and September 25, 2009,

[6] The contractor needed to contact URE personnel to receive the necessary access code from the Secure ID token in order to remotely access the URE system. This transfer of the access code was not functioning and URE could not remedy the issue in time for the contractor to complete training.

respectively. Although URE timely revoked the authorized unescorted physical access of both individuals, cyber access was not revoked until June 15, 2009 and October 7, 2009 respectively.

Reliability*First* concluded that URE was (1) in violation of CIP-004-1 R2.3 for its failure to provide documentation that a contractor with cyber access to Critical Cyber Assets completed annual cyber security training in 2009; and (2) in violation of CIP-004-1 R4.2 for its failure to revoke, within seven calendar days, access to Cyber Security Assets for 3 individuals who no longer required such access.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the CIP-004-1 R2.3 violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because (1) the contractor's access to URE's energy control system was restricted; (2) the contractor in question had completed a Personnel Risk Assessment; and (3) the contractor, in 2008, had completed the initial cyber-security training required for access to be granted. In addition, the contractor did not access the energy control system from June 2009 through March 24, 2010, when URE revoked his cyber access.

With regard to the CIP-004-1 R4.2 violation, Reliability*First* determined that the subject violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS because, at no time did any of the three individuals have full access to Cyber Security Assets after such access was no longer required and because the full revocation of cyber and/or physical access was exceeded by, at most, five calendar days. Additionally, the two contractors that retired did not have remote electronic access to URE's Critical Cyber Assets and since both of the contractors had their authorized physical assess revoked, they could not remotely access the URE system.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATES **R2.3: 6/30/09 (the date on which the contractor was due to receive annual training) through 3/24/10 (the date on which URE revoked the contractor's cyber access)**
R4.2: 7/1/08 (when URE was required to be compliant with CIP-004-1 R4.2 as a Table 1 entity for its system control center) through 3/1/11 (Mitigation Plan completion)

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

ARE THE VIOLATIONS 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 FOR **CIP-004-1 R2.3**:

MITIGATION PLAN NO.	**MIT-10-3207**
DATE SUBMITTED TO REGIONAL ENTITY	**11/10/10**
DATE ACCEPTED BY REGIONAL ENTITY	**11/30/10**
DATE APPROVED BY NERC	**1/10/11**
DATE PROVIDED TO FERC	**1/10/11**

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	**7/30/10**
DATE OF CERTIFICATION LETTER	**11/10/10**[7]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**7/30/10**
DATE OF VERIFICATION LETTER	**4/25/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**7/30/10**

[7] The Certification of Completion document was signed on November 13, 2010.

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

1. **URE has reemphasized the need to follow and implement correctly URE's security training process to personnel in the organization who conduct and monitor annual training.**
2. **URE created a centralized electronic reporting and alerting application to signal to responsible personnel that an individual is nearing the deadline for annual training. The information provided by the application will flag the individuals need for training and will notify the responsible organization to initiate the revocation process for the individual, if necessary.**

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)

- **A document that provides evidence that meetings were held with URE personnel to discuss the personnel security training process.**
- **A document that provides evidence that URE created a centralized electronic reporting application that on a daily basis will query a variety of access list databases looking for any changes that occurred in the last day.**
- **A document provides an explanation of the message which appeared in the document above. The message appeared to indicate that the system was not being queried to check if all personnel with CCA access had the required training. This document explains that the LMS database records are uploaded manually on at least a quarterly basis and that the centralized electronic reporting application will check the file on that specific day and that the LMS file was not present on the days the examples were given.**

FOR FINAL ACCEPTED MITIGATION PLAN FOR **CIP-004-1 R4.2**:

MITIGATION PLAN NO.	**MIT-09-3208**
DATE SUBMITTED TO REGIONAL ENTITY	**11/10/10**
DATE ACCEPTED BY REGIONAL ENTITY	**11/30/10**
DATE APPROVED BY NERC	**1/10/11**
DATE PROVIDED TO FERC	**1/10/11**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**3/1/11**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**3/1/11**

DATE OF CERTIFICATION LETTER **4/12/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **3/1/11**

DATE OF VERIFICATION LETTER **4/25/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **3/1/11**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

1. **URE is now performing the existing revocation process with the necessary focus toward obtaining necessary permission and actual revocation of access within the required timeframe. One person is now charged to monitor the entire process;**
2. **URE will conduct a thorough review of the current access revocation process to address the gaps applicable to the subject violations as well as other process improvements identified during meetings with subject matter experts and the groups who have responsibility for the performance of the process; and**
3. **URE will include the following in the process review and redesign**
    a. **Determine an appropriate work flow to perform the actual revocation of access;**
    b. **Obtain timely revocation approvals;**
    c. **Start a revocation process timer to indicate to the active participants that the revocation process has begun and when completion is required; and**
    d. **Work flow to log when the revocation process has begun and has successfully been completed.**

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)

- **A document that provides evidence that meetings were held with process stakeholders to determine improvements to the revocation process.**
- **A document that provides a flowchart of the new revocation process.**
- **A document that provides an actual example of revoking electronic access for an employee who changed positions at URE.**
- **A document that provides evidence that the URE CIP application ran at 2:01 AM on March 29, 2011 and correctly detected that the access changes for this employee occurred.**

EXHIBITS:

SOURCE DOCUMENT
Reliability*First*'s Summaries of Possible Violation for CIP-004-1 R2.3 and R4.2

MITIGATION PLAN
URE's Mitigation Plan, designated as MIT-10-3207, for CIP-004-1 R2.3, dated November 10, 2010
URE's Mitigation Plan, designated as MIT-09-3208, for CIP-004-1 R4.2, dated November 10, 2010

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-004-1 R2.3, dated November 10, 2010
URE's Certification of Mitigation Plan Completion for CIP-004-1 R4.2, dated April 12, 2011

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R2.3, dated April 25, 2011
Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R4.2, dated April 25, 2011

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-006-1 R1.8

DISPOSITION OF VIOLATION
Dated March 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC200900232	**RFC200900232**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-006-1	**1**	**1.8**	**Lower**[1]	**N/A**[2]

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

The purpose statement of CIP-006-1 provides in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."

CIP-006-1 R1 states, in pertinent part:

> **R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:**
>
> *******
>
> **R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.**

VIOLATION DESCRIPTION

On December 20, 2009, URE self-reported violations CIP-006-1, R1.8 and CIP-007-1, R1 after it discovered that it did not test security patches for Cyber Assets used in the access control and monitoring of the Physical Security Perimeter prior to such patches entering the production environment and that it failed to follow its change

[1] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; R1.7 and R1.8 each have a "Lower" VRF.
[2] VSLs were not in effect during the duration of the subject violation.

management procedures. Upon review of the self-report, Reliability*First* determined that the self-report identified only a non-compliance with CIP-006-1, R1.8. Accordingly, the CIP-007-1 R1 violation was subsequently dismissed as CIP-007-1 R1 is not applicable to the security guard workstations discussed in the self-report because they are not within an Electronic Security Perimeter.

URE uses automated security patch software to update its corporate computers not subject to the CIP Reliability Standards. As Cyber Assets used in the access control and monitoring of the Physical Security Perimeter, URE's security guard workstations, however, are not meant to receive security patches until URE ensures that the changes meet the testing and change management requirements in URE's security policies established in accordance with CIP-007-1. URE's security software, due to database corruption, did not recognize that the security guards' workstations should have been excluded from receiving automatic security patch software. As a result of this database corruption, URE delivered a new set of security patches to the security guards' workstations without URE completing testing on those patches.

Reliability*First* alleges that, since URE designates the security guard workstations as Cyber Assets used in the access control and monitoring of the Physical Security Perimeter, URE's failure to test these security patches constitutes a violation of the subject Standards requirement.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that subject violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the affected security guard workstations are connected to the URE corporate network, which is protected by firewalls and monitored intrusion detection systems.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATES

8/12/2009 (when the security guard workstations were reclassified in the software to install security patches without the requisite testing) through 11/3/10 (Mitigation Plan completion)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **12/23/09**

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-3122**
DATE SUBMITTED TO REGIONAL ENTITY	**11/10/10**
DATE ACCEPTED BY REGIONAL ENTITY	**11/22/10**
DATE APPROVED BY NERC	**12/14/10**
DATE PROVIDED TO FERC	**12/16/10**

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	**11/3/10**
DATE OF CERTIFICATION LETTER	**11/10/10**[3]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**11/3/10**
DATE OF VERIFICATION LETTER	**4/21/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**11/3/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

1. **Meetings with internal and with vendor representatives;**
2. **resolution/repair of vendor database corruption; and**
3. **E-mail sent to Security Guards to be aware of the vendor screen and to notify the URE Help Desk should it appear.**

[3] The Certification of Completion document was signed on November 13, 2010.

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

- **URE submitted an Adobe scanned service request.**
- **Resolution/repair of vendor database corruption URE submitted an Adobe scanned service request log.**
- **E-mail sent to Security Guards to be aware of the vendor screen and to notify the URE Help Desk should it appear URE submitted an Adobe scanned email thread sent to a number of URE personnel (position or function in URE was not noted), from URE/Security.**

EXHIBITS:

SOURCE DOCUMENT
URE's self-report for CIP-006-1 R1.8 dated December 20, 2009

MITIGATION PLAN
URE's Mitigation Plan, designated as MIT-09-3122, dated November 10, 2010

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-006-1 R1.8, dated November 10, 2010

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-1 R1.8, dated April 12, 2011