**PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 28, 2011

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Documents (Attachment e), 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-006-1 Requirement (R)5, CIP-005-1 R2.6, CIP-004-1 R4, CIP-006-1 R5, and CIP-006-1 R3. 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. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers RFC201000332, RFC201000378, RFC201000678,

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

[2] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

RFC201000679, and RFC201000680 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 3, 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-759 | RFC201000332 | CIP-006-1 | 5 | Lower | 3/6/10-3/31/10 | 15,000 |
| | RFC201000378 | CIP-005-1 | 2.6 | Lower[3] | 1/1/10-5/14/10 | |
| | RFC201000678 | CIP-004-1 | 4 | Lower[4] | 1/1/10-8/23/10 | |
| | RFC201000679 | CIP-006-1 | 5 | Lower | 1/1/10-4/30/10 | |
| | RFC201000680 | CIP-006-1 | 3 | Medium[5] | 1/1/10-9/15/10 | |

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

CIP-006-1 R5 - OVERVIEW

URE submitted a Violation Self-Reporting form. Reliability*First* determined that URE did not retain physical access logs from March 8, 2010 to March 31, 2010, as required by CIP-006-1 R5, due to technical problems and network connectivity failure with one of its access card readers controlling access to physical security perimeters in its corporate headquarters.

CIP-005-1 R2.6 - OVERVIEW

URE submitted a Self-Report. Reliability*First* determined that URE omitted a command when configuring its electronic access control devices, which resulted in 13 out of 17 devices not displaying an Appropriate Use Banner on the user screen upon all interactive access attempts, in violation of CIP-005-1 R2.6.

[3] CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" Violation Risk Factor (VRF); R2.5 and its sub-requirements and R2.6 each have a "Lower" VRF.
[4] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF.
[5] CIP-006-1 R3 and R3.1 each have a "Medium" VRF and CIP-006-1 R3.2 has a "Lower" VRF.

CIP-004-1 R4 - OVERVIEW
URE disclosed this violation in a draft mitigation plan. A couple of months later, at Reliability*First*'s request, URE sent Reliability*First* a letter memorializing several non-compliances. Reliability*First* determined that URE improperly configured an access badge reader in a freight elevator that stops at the floor housing Critical Cyber Assets. This error enabled 20 unauthorized personnel to have unescorted physical access. URE failed to list these individuals as having unescorted physical access to Critical Cyber Assets and failed to include seven other individuals with authorized unescorted access to Critical Cyber Assets on its access list, one of those seven did not have access reviewed in the first and second quarter of 2010. URE violated CIP-004-1 R4 based on these errors.

CIP-006-1 R5 - OVERVIEW
URE disclosed this violation in a draft mitigation plan. A couple of months later, at Reliability*First*'s request, URE sent Reliability*First* a letter memorializing several non-compliances. Reliability*First* determined that URE was unable to distinguish between individuals' access to a floor containing Critical Cyber Assets and four other floors via a freight elevator and therefore URE failed to retain access logs, as required by CIP-006-1 R5.

CIP-006-1 R3 - OVERVIEW
URE disclosed this violation in a draft mitigation plan. A couple of months later, at Reliability*First*'s request, URE sent Reliability*First* a letter memorializing several non-compliances. Reliability*First* determined that URE did not monitor access to locked racks securing data communications cables running to the floor housing Critical Cyber Assets from URE's electric System Operations Center continuously, 24 hours per day, seven days per week, as required by CIP-006-1 R3.

**Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed**[6]

**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,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on June 10, 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.

[6] *See* 18 C.F.R. § 39.7(d)(4).
[7] *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).

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

1. the violations constituted URE's first occurrence of violation of the subject NERC Reliability Standards;[8]
2. URE self-reported the violations;
3. Reliability*First* reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation 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 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.

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.

**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.

[8] Although there are two violations of CIP-006-1 R5, URE discovered the second occurrence in the course of the investigation of the first. Therefore, Reliability*First* did not consider URE's first violation to be an aggravating factor.

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 parts of this NOP are the following documents:

a) Settlement Agreement by and between Reliability*First* and URE executed January 3, 2011, included as Attachment a;

   i. Violation Self-Reporting Form for CIP-006-1 R5, included as Attachment A to the Settlement Agreement;

   ii. Violation Self-Reporting Form for CIP-005-1 R2.6, included as Attachment B to the Settlement Agreement;

   iii. Disclosure Letter for CIP-004-1 R4, CIP-006-1 R3, and CIP-006-1 R5, included as Attachment C to the Settlement Agreement;

   iv. Mitigation Plan Submittal Form for CIP-006-1 R5, included as Attachment D to the Settlement Agreement;

   v. Certification of Mitigation Plan Completion for CIP-006-1 R5, included as Attachment E to the Settlement Agreement;

   vi. Mitigation Plan Submittal Form for CIP-005-1 R2.6, included as Attachment F to the Settlement Agreement;

   vii. Certification of Mitigation Plan Completion for CIP-005-1 R2.6, included as Attachment G to the Settlement Agreement;

   viii. Mitigation Plan Submittal Form for CIP-004-1 R4, CIP-006-1 R3, and CIP-006-1 R5, included as Attachment H to the Settlement Agreement; and

   ix. Certification of Mitigation Plan Completion for CIP-004-1 R4, CIP-006-1 R3, and CIP-006-1 R5, included as Attachment I to the Settlement Agreement;

b) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-1 R5, included as Attachment b;

c) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-005-1 R2.6, included as Attachment c;

d) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R4, CIP-006-1 R3, and CIP-006-1 R5, included as Attachment d; and

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

   i. Disposition Document for CIP-004-1 R4, included as Attachment e.1;

   ii. Disposition Document for CIP-005-1 R2.6, included as Attachment e.2; and

   iii. Disposition Document for CIP-006-1 R3, and R5 (two instances), included as Attachment e.3.

**A Form of Notice Suitable for Publication**[9]

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

**Notices and Communications**

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

| | |
|---|---|
| Gerald W. Cauley<br>President and Chief Executive Officer<br>David N. Cook*<br>Sr. Vice President and General Counsel<br>North American Electric Reliability Corporation<br>116-390 Village Boulevard<br>Princeton, NJ 08540-5721<br>(609) 452-8060<br>(609) 452-9550 – facsimile<br>david.cook@nerc.net<br><br>Michael D. Austin*<br>Associate Attorney<br>Reliability*First* Corporation<br>320 Springside Drive, Suite 300<br>Akron, OH 44333<br>(330) 456-2488<br>mike.austin@rfirst.org<br><br>*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*<br>Associate General Counsel for Regulatory and Corporate Matters<br>Davis Smith*<br>Attorney<br>North American Electric Reliability Corporation<br>1120 G Street, N.W.<br>Suite 990<br>Washington, DC 20005-3801<br>(202) 393-3998<br>(202) 393-3955 – facsimile<br>rebecca.michael@nerc.net<br>davis.smith@nerc.net<br><br>Robert K. Wargo*<br>Director of Enforcement and Regulatory Affairs<br>Reliability*First* Corporation<br>320 Springside Drive, Suite 300<br>Akron, OH 44333<br>(330) 456-2488<br>bob.wargo@rfirst.org<br><br>L. Jason Blake*<br>Corporate Counsel<br>Reliability*First* Corporation<br>320 Springside Drive, Suite 300<br>Akron, OH 44333<br>(330) 456-2488<br>jason.blake@rfirst.org |

[9] *See* 18 C.F.R. § 39.7(d)(6).

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 Regulatory and Corporate Matters
Davis Smith
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
davis.smith@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Attachment e

# Disposition Document for Common Information

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment e

# DISPOSITION OF VIOLATION[1]

**INFORMATION COMMON TO INSTANT VIOLATIONS**
**Dated June 10, 2011**

| REGISTERED ENTITY | NERC REGISTRY ID | NOC# |
|---|---|---|
| **Unidentified Registered Entity (URE)** | **NCRXXXXX** | **NOC-759** |

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 **FIVE** VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

**Although there were two violations of one Standard and Requirement, URE discovered the second violation in the course of the investigation of the first.**

[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.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION


**Therefore, Reliability*First* did not consider URE's first violation to be an aggravating factor.**

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* favorably considered certain aspects of URE's internal compliance program to be mitigating factors in determining the penalty amount.**

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

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION


(5) ANY EVIDENCE THE VIOLATION(S) WERE INTENTIONAL (IF THE RESPONSE IS "YES," THE ABBREVIATED NOP FORM MAY NOT BE USED.)

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

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

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **11/11/2010** 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 ☐ DID NOT CONTEST ☒
HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-004-1 R4

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBILC VERSION
Attachment e.1

# DISPOSITION OF VIOLATION
## Dated June 10, 2011

NERC TRACKING NO. **RFC201000678**

REGIONAL ENTITY TRACKING NO. **300729**

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-004-1** | **4** | | **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-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 R4 states in pertinent part:**

> **R4.** Access—The Responsible Entity[3] 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.

(Footnote added.)

[1] CIP-004-1 R4 and R4.1 each have a "Lower" Violation Risk Factor (VRF); R4.2 has a "Medium" VRF.
[2] 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.
[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 Reliability Organizations.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBILC VERSION


VIOLATION DESCRIPTION

URE disclosed these violations in a draft mitigation plan. At Reliability*First*'s request, URE sent Reliability*First* a letter memorializing several non-compliances (the Letter). According to the Letter, a floor of URE's headquarters is within a physical security perimeter because the floor houses Critical Cyber Assets. In order to control access to this floor, URE installed an access badge reader in a freight elevator. URE improperly configured the access badge reader, thereby enabling 20 unauthorized personnel to have unescorted physical access to this floor. URE failed to list these individuals as having unescorted physical access to Critical Cyber Assets in violation of CIP-004-1 R4.

Also according to the Letter, physically-secured data communications cables running to the referenced floor from URE's electric system operations center passed through two locked racks in the URE's information technology data center. URE granted unescorted physical access to these locked racks to six individuals, but failed to include these individuals' physical access on its access lists maintained in accordance with CIP-004-1 R4. URE granted these six individuals physical access to the locked racks because these six individuals already had been properly granted cyber access to Critical Cyber Assets.

Finally, URE failed to include one individual with authorized unescorted access to Critical Cyber Assets on the referenced floor of URE's headquarters on its access list. As a result, URE failed to review this individual's access for the first and second quarter of 2010.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because all of the individuals who could have gained access to the referenced floor had current personnel risk assessments, and four of the individuals had completed NERC CIP training. There is no evidence based upon interviews and job assignment analysis that any of the individuals ever accessed this floor. In addition, the only individuals to access the two locked racks were already granted cyber access to Critical Cyber Assets, and had completed training and a satisfactory personnel risk assessment.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBILC VERSION


## II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **Self-Report**

DURATION DATE(S) 1/1/10 through 8/23/10 (when URE changed the access procedures for the two locked racks)

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

| | |
|---|---|
| MITIGATION PLAN NO. | **MIT-10-3213** |
| DATE SUBMITTED TO REGIONAL ENTITY | **11/23/10** |
| DATE ACCEPTED BY REGIONAL ENTITY | **12/22/10** |
| DATE APPROVED BY NERC | **1/26/11** |
| DATE PROVIDED TO FERC | **1/27/11** |

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **12/31/10**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **12/22/10**

| | |
|---|---|
| DATE OF CERTIFICATION LETTER | **12/30/10** |
| CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF | **12/22/10** |

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBILC VERSION


DATE OF VERIFICATION LETTER **7/25/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **12/22/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE removed access to the referenced floor for all 20 individuals involved. URE also redesigned and rebuilt the floor so that there is no access to the six wall perimeter *via* the freight elevator. The new perimeter encompasses a smaller area, reducing the number of individuals accessing it regularly. The freight elevator is no longer contained within the six wall perimeter. URE also put in place a procedure to sign in any individual accessing this floor *via* the freight elevator. URE changed its procedures for accessing the racks in the IT Data Center, requiring an individual with authorized physical access to control the key to the locked racks. Finally, URE implemented badge access control on the racks and supplemental video camera monitoring.

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)

- **An Excel file that contains extracted data from the badge access system activity log. The file shows the access for the 20 cleaning individuals was removed on July 7, 2010 by changing the department code from 17 to zero.**
- **A copy of an internal web site noting a revised process for granting and approving access to Physical Security Perimeters.**
- **An internal memorandum indicating the CCA floor has been redesigned and new access points to the Physical Security Perimeters are in effect.**
- **A layout of the redesigned CCA floor noting the newly established Physical Security Perimeters and access points into the perimeters.**

EXHIBITS:

SOURCE DOCUMENT
Disclosure Letter for CIP-004-1 R4

MITIGATION PLAN
Mitigation Plan Submittal Form for CIP-004-1 R4

CERTIFICATION BY REGISTERED ENTITY
Certification of Mitigation Plan Completion for CIP-004-1 R4, CIP-006-1 R3, and CIP-006-1 R5

VERIFICATION BY REGIONAL ENTITY
Verification of Mitigation Plan Completion for CIP-004-1 R4, CIP-006-1 R3, and CIP-006-1 R5

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-005-1 R2.6

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment e.2

# DISPOSITION OF VIOLATION
**Dated June 10, 2011**

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC201000378** | **RFC201000378** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-005-1** | **2** | **2.6** | **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-005-1 provides in pertinent part: "**Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.**"**

**CIP-005-1 R2 states in pertinent part:**

> **R2.** Electronic Access Controls — The Responsible Entity[3] shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> ***
>
> **R2.6.** Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

(Footnote Added.)

[1] CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" Violation Risk Factor (VRF); R2.5 and its sub-requirements and R2.6 each have a "Lower" VRF.
[2] At the time of the violations, no VSLs were in effect for CIP-005-1. 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.
[3] Within the text of Standard CIP-005, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION


VIOLATION DESCRIPTION

URE submitted a Violation Self-Reporting form identifying non-compliance with CIP-005-1 R2.6. URE determined that not all electronic access control devices displayed the requisite Appropriate Use Banner in accordance with CIP-005-1 R2.6. Of URE's 17 electronic access control devices, 13 did not display the banner. URE's subsequent internal investigation revealed that the team responsible for configuring the devices omitted a command resulting in the 13 devices failing to display the requisite Appropriate Use Banner. The network technicians responsible for the oversight leading to the possible alleged violation were subsequently retrained on the relevant processes and procedures.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because only ten information technology employees could access the ports that did not display the Appropriate Use Banner. These individuals were aware of the content of the Appropriate Use Banner and URE's security standards, and all had undergone personnel risk assessments and training. URE also maintains 12-character password authentication on all affected devices, and access through these devices does not provide direct access to the software that monitors and controls the bulk electric system. The implicated assets were a small subset of URE's overall population of CCAs, and this small subset does not directly monitor or control the BES. The potential risk was further reduced because this subset was only used by IT employees, not BES operators.

## II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **Self-Report**

DURATION DATE(S) 1/1/10 through 5/14/10 (when the required Appropriate Use Banner was displayed on all devices)[4]

[4] The Self-Report incorrectly states that the violation was ended on May 12, 2010.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION


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-10-2804** |
| DATE SUBMITTED TO REGIONAL ENTITY | **8/06/10** |
| DATE ACCEPTED BY REGIONAL ENTITY | **9/02/10** |
| DATE APPROVED BY NERC | **9/08/10** |
| DATE PROVIDED TO FERC | **9/08/10** |

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **5/26/10**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **5/26/10**

DATE OF CERTIFICATION LETTER **12/20/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **5/26/10**

DATE OF VERIFICATION LETTER **1/20/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **5/26/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE mitigated the violation by configuring all devices to display the Appropriate Use Banner, and implementing a continual compliance check that runs whenever configuration changes occur, or twice per week at a minimum. This compliance check verifies documented usernames and the existence of the Banner. URE also provided training to network technicians to review CIP processes and procedures.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment e.2

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)

- Electronic Security Perimeters procedure
- Screenshots of Banners on 13 Devices, no dates listed.
- Screenshot of configuration verification

EXHIBITS:

SOURCE DOCUMENT
Violation Self-Reporting Form for CIP-005-1 R2.6

MITIGATION PLAN
Mitigation Plan Submittal Form MIT-10-2804 for CIP-005-1 R2.6

CERTIFICATION BY REGISTERED ENTITY
Certification of Mitigation Plan Completion for CIP-005-1 R2.6

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion for CIP-005-1 R2.6

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-006-1 R3, and R5 (two instances)

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment e.3

# DISPOSITION OF VIOLATION
**Dated June 10, 2011**

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC201000332** | **RFC201000332** |
| **RFC201000679** | **300730** |
| **RFC201000680** | **300731** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S)[1] |
|---|---|---|---|---|
| **CIP-006-1** | **5** | | Lower | N/A |
| **CIP-006-1** | **5** | | Lower | N/A |
| **CIP-006-1** | **3** | | Medium[2] | N/A |

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

**The purpose statement of CIP-006 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 R5 states:"** Access Log Retention — The responsible entity[3] shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008." (Footnote added.)

**CIP-006-1 R3 states:**

> **R3.** Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized

[1] At the time of the violations, no Violation Severity Levels (VSLs) were in effect for CIP-006-1. 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.
[2] CIP-006-1 R3 and R3.1 each have a "Medium" Violation Risk Factor (VRF) and CIP-006-1 R3.2 has a "Lower" VRF.
[3] Within the text of Standard CIP-006, "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.

access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:

R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

VIOLATION DESCRIPTION

**CIP-006-1 R5-RFC201000332**

URE submitted a Self-Report identifying non-compliance with CIP-006-1 R5. While investigating a report of unrelated problems with a card reader on March 31, 2010, URE found that it failed to retain physical access logs from March 8, 2010 to March 31, 2010 due to technical problems with one of its access card readers. Additionally, the redundant local access logs, which were stored on the access card reader itself, were not maintained during this time period. URE discovered that the card reader device continued to locally collect access log data; however, it ran out of memory on March 8, 2010 and therefore could not collect any additional physical access logs.

URE also discovered that its corporate security badge access system did not have access log data from March 6, 2010 through March 31, 2010 due to a network connectivity failure between the location of the relevant card readers and the centralized URE's corporate security servers.

Therefore, URE failed to retain its physical access logs for at least 90 calendar days, as required by the Standard.

**CIP-006-1 R5-RFC201000679**

URE disclosed these violations in a draft mitigation plan. In a Letter, at Reliability*First*'s request, URE identified a possible non-compliance with CIP-006-1 R5. According to the Letter, a floor of URE's headquarters is within a Physical Security Perimeter (PSP) because this floor houses Critical Cyber Assets (CCAs). URE maintained controls limiting access to this floor to authorized personnel via an access card reader in a freight elevator. These access records logged individuals' access to four other floors via the same freight elevator and access card reader, without delineating precisely which floor the individual accessed. The other floors are not within the PSPs. Because URE was unable to distinguish between individuals' access to the referenced

CCA floor and the four other floors, URE failed to retain access logs in accordance with CIP-006-1 R5.

**CIP-006-1 R3-RFC201000680**

In the Letter, URE identified non-compliance with CIP-006-1 R3. Physically secured data communications cables running to the referenced floor from URE's electric system operations center passed through two locked racks in the URE's information technology data center. URE restricted access to these locked racks by restricting the number of keys granted for these racks. URE, however, failed to monitor access to these locked racks continuously, 24 hours per day, seven days per week in accordance with CIP-006-1 R3.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:

**CIP-006-1 R5-RFC201000332**

Although the card reader failed to log access data for a period of time, the card reader still restricted access to the PSP. In addition, URE maintains a video monitoring and recording system that enables visual identification of individuals who access, or attempt to access, the PSP.

**CIP-006-1 R5-RFC201000679**

Although access records may not have been recorded in detail, only authorized individuals could have accessed the referenced floor. These authorized individuals were properly background-checked and trained. From a cyber viewpoint, the risk to the BPS and security was minimal because anyone gaining physical access would still need valid credentials to log on to any of the NERC CIP-protected systems. Attempts to infiltrate the network using force would have been immediately detected by the network monitoring system for appropriate response.

**CIP-006-1 R3-RFC201000680**

The information technology data center itself has restricted access, and it is monitored by operators 24 hours a day. Additionally, URE restricted access to the keys for the two racks in question.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION


## II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

**CIP-006-1, R5-RFC201000332:** Self-Report
**CIP-006-1 R5-RFC201000679 and CIP-006-1 R3-RFC201000680:** Self-Report

DURATION DATE(S)

**CIP-006-1 R5-RFC201000332**

3/6/10 (when the card access reader stopped logging access data) through 3/31/10 (when URE enabled an alternate method of logging access data to ensure that access data was being collected)

**CIP-006-1 R5-RFC201000679**

1/1/10 through 4/30/10 (when URE put in place a procedure requiring any individual to sign in when accessing the CCA floor *via* the freight elevator).

**CIP-006-1 R3-RFC201000680**

1/1/10 through 9/15/10 (when URE took steps to change the procedure for accessing the racks in the IT Data Center).

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

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION


## III. MITIGATION INFORMATION

**CIP-006-1 R5-RFC201000332:**

FOR FINAL ACCEPTED MITIGATION PLAN:

| | |
|---|---|
| MITIGATION PLAN NO. | **MIT-10-3022** |
| DATE SUBMITTED TO REGIONAL ENTITY | **10/12/10** |
| DATE ACCEPTED BY REGIONAL ENTITY | **10/26/10** |
| DATE APPROVED BY NERC | **11/17/10** |
| DATE PROVIDED TO FERC | **11/19/10** |

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **12/20/10**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **12/20/10**

| | |
|---|---|
| DATE OF CERTIFICATION LETTER | **12/20/10** |
| CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF | **12/20/10** |
| DATE OF VERIFICATION LETTER | **6/3/11** |
| VERIFIED COMPLETE BY REGIONAL ENTITY AS OF | **12/20/10** |

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE mitigated the alleged violation and collected access log data by other means until the underlying problem was corrected. On March 31, 2010, URE posted two security guards at the affected access point to manually verify authorization and log access until the electronic system was restored later that day. Also on March 31, 2010, the issue was mitigated by ensuring the accuracy of router rules, and the badge access was tested to verify the badge access systems were sending changes to the card reader.

URE's Security Manger conducted additional operator training reinforcing reporting of connectivity issues in regard to any NERC CIP location. This action was completed on April 22, 2010.

URE conducted a review on business days of the Badge Access System for connectivity issues to NERC CIP sites. This action was completed on May 14, 2010.

URE's Security Manger started running weekly controller offline alarm reports to track historical controller connectivity alarms. This action was completed on April 12, 2010.

NERC controllers that should be considered designated cyber assets as part of the badge access system (NERC CIP network) have been identified and were included in the system. This action was completed on December 20, 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)

- **Scanned copy of the badge system, which verifies that the last access events logged by the system were on March 6, 2010**
- **A copy of an e-mail requesting two guards be posted at the glass doors on the CCA floor entrance.**
- **A copy of an e-mail stating that the static route was placed on the core switch, which resolves the issue of not recording badge access events.**
- **A copy of an e-mail stating that the badge access logs to the CCA floor have been recovered as of the date of the correction to the badge access system.**
- **A copy of an e-mail stating that instructions were supplied by the vendor on how to recognize and report the badge access connectivity issues to mitigate further recurrence of the violation.**
- **A screenshot of a document from the vendor providing an example of a daily checklist to monitor the badge access system.**
- **A copy of the weekly calendar which indicates several meeting on various days during which net controllers were identified and subsequently documented in the entity's SharePoint system.**
- **A photograph of a device and bearing a sticker indicating the device is protected under NERC CIP.**

**CIP-006-1 R5-RFC201000679 and CIP-006-1 R3-RFC201000680:**

FOR FINAL ACCEPTED MITIGATION PLAN:

| | |
|---|---|
| MITIGATION PLAN NO. | **MIT-10-3213**[4] |
| DATE SUBMITTED TO REGIONAL ENTITY | **11/23/10** |
| DATE ACCEPTED BY REGIONAL ENTITY | **12/22/10** |
| DATE APPROVED BY NERC | **1/26/11** |
| DATE PROVIDED TO FERC | **1/27/11** |

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

[4] The CIP-004-1 R4 (RFC201000678) violation is also included in this Mitigation Plan and is being addressed in its own disposition document.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION


**CIP-006-1 R5-RFC201000679:**

EXPECTED COMPLETION DATE **11/11/10**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **12/22/10**

DATE OF CERTIFICATION LETTER **12/30/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **12/22/10**

DATE OF VERIFICATION LETTER **7/25/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **12/22/10**

**CIP-006-1 R3-RFC201000680:**

EXPECTED COMPLETION DATE **10/31/10**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **10/31/10**

DATE OF CERTIFICATION LETTER **12/30/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **10/31/10**

DATE OF VERIFICATION LETTER **7/25/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **10/31/10**

**CIP-006-1 R5-RFC201000679 and CIP-006-1 R3-RFC201000680:**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE removed access to the referenced floor for all 20 individuals. URE also redesigned and rebuilt this floor so that there is no access to the six wall perimeter *via* the freight elevator. The new perimeter encompasses a smaller area, reducing the number of individuals accessing it regularly. The freight elevator is no longer contained within the six wall perimeter. URE also put in place a procedure to sign in any individual accessing the CCA floor *via* the freight elevator.

URE changed its procedures for accessing the racks in the IT Data Center, requiring an individual with authorized physical access to control the key to the locked racks. Finally, URE implemented badge access control on the racks and supplemental video camera monitoring.

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)

**CIP-006-1 R5-RFC201000679:**

- **Ref 6 - RFC201000679 Put in a procedure to sign in any individual accessing this floor via the freight elevator on April 30, 2010.**

- **Ref 7 - RFC201000679 Reconstruct the CCA floor so the freight elevator is not contained within the new six-wall perimeter dated November 11, 2010.**

**CIP-006-1 R3-RFC201000680:**

- **Ref 8 - RFC201000680 Procedures have been changed for approving access to the racks in the IT Data Center on September 15, 2010.**
- **Ref 9 - RFC201000680 Badge access control was implemented and supplemental video for monitoring the IT Data Center Equipment racks on October 31, 2010.**

EXHIBITS:

**CIP-006-1, R5-RFC201000332:**

SOURCE DOCUMENT
Violation Self-Reporting Form for CIP-006-1 R5

MITIGATION PLAN
Mitigation Plan Submittal Form MIT-10-3022 for CIP-006-1 R5

CERTIFICATION BY REGISTERED ENTITY
Certification of Mitigation Plan Completion for CIP-006-1 R5

VERIFICATION BY REGIONAL ENTITY
Verification of Mitigation Plan Completion for CIP-006-1 R5

**CIP-006-1 R5-RFC201000679 and CIP-006-1 R3-RFC201000680:**

SOURCE DOCUMENT
Disclosure Letter for CIP-006-1 R3, and CIP-006-1 R5

MITIGATION PLAN
Mitigation Plan Submittal Form MIT-10-3213for CIP-006-1 R3, and CIP-006-1 R5

CERTIFICATION BY REGISTERED ENTITY
Certification of Mitigation Plan Completion for CIP-006-1 R3, and CIP-006-1 R5

VERIFICATION BY REGIONAL ENTITY
Verification of Mitigation Plan Completion for CIP-006-1 R3, and CIP-006-1 R5