PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

June 29, 2011

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Documents (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, R4.2; CIP-006-1, R1.2; CIP-006-1, R3; CIP-006-1, R1.8 and CIP-006-2, R2.2; CIP-007-1 and CIP-007-2a, R6; CIP-006-2c, R4, R5, and R6; and CIP-006-3c, R4, R5, and R6. According to the Settlement Agreement, URE neither admits nor denies the violation, but has agreed to the assessed penalty of eighty-five thousand dollars ($85,000), 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

[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

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Violation Tracking Identification Numbers RFC201000234, RFC201000240, RFC201000241, RFC201000295, RFC201000432, RFC201000435, RFC201000658, RFC201000659, RFC201000660, RFC201000681, RFC201000682, and RFC201000683 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 February 24, 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[3]	Total Penalty ($)
NOC-820	RFC201000234 RFC201000240	CIP-004-1	4.2	Medium[4]	1/1/10-1/12/10	85,000
					1/1/10-1/21/10	
	RFC201000241	CIP-006-1	1.2	Medium[5]	1/1/10-1/22/10	
	RFC201000295	CIP-006-1	3	Medium[6]	1/1/10-3/5/10	
	RFC201000432	CIP-006-1/ CIP-006-2[7]	1.8/2.2	Lower[8]	1/31/10-6/29/10	
	RFC201000435	CIP-007-1/ CIP-007-2a[9]	6, 6.4	Lower	2/15/10-9/17/10	

[3] URE is a "Table 3" entity under the NERC implementation plan for CIP standards CIP-002-1 through CIP-009-1.
[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, R1.8 and R1.9 each have a "Lower" VRF.
[6] CIP-006-1 R3, R3.1 and R3.2 each have a "Medium" VRF and R3.3 has a "Lower" VRF.
[7] CIP-006-1 became effective on January 1, 2010 for "Table 3" entities and was superseded by CIP-006-2 on April 1, 2010. URE's violation included instances that occurred both before and after April 1, 2010. When CIP-006-2 became effective, the "Cyber Assets used in the access control and monitoring of the Physical Security Perimeter" from CIP-006-1 R1.8 became "Cyber Assets that authorize and/or log access to the Physical Security Perimeter" in CIP-006-2 R2. The Settlement Agreement uses the terminology from CIP-006-1 R1.8 throughout, and where applicable, it designates the language from CIP-006-2 R2.2.
[8] The VRF for CIP-006-2 R2.2 is "Medium" which became effective on April 1, 2010.
[9] URE violated the standard from February 15, 2010 to September 17, 2010. CIP-007-1 became effective on January 1, 2010, which was superseded by CIP-007-2 on April 1, 2010. All relevant portions of CIP-007-2a R6 are exactly the same as CIP-007-1 R6.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration[3]	Total Penalty ($)
	RFC201000658	CIP-006-2c	4	Medium	9/15/10-9/17/10	
	RFC201000659	CIP-006-2c	5	Medium	9/15/10-9/17/10	
	RFC201000660	CIP-006-2c	6	Lower	9/15/10-9/17/10	
	RFC201000681	CIP-006-3c	4	Medium	10/19/10-10/20/10	
	RFC201000682	CIP-006-3c	5	Medium	10/19/10-10/20/10	
	RFC201000683	CIP-006-3c	6	Lower	10/19/10-10/20/10	

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 R4.2 RFC201000234 and RFC201000240 - OVERVIEW

URE submitted a Self-Report to Reliability*First* identifying the RFC201000234 violation and as part of its investigation and mitigating actions; URE conducted a manual review of all employees with unauthorized physical access to CCAs. As a result of this review, URE submitted a Self-Report to Reliability*First* identifying the RFC201000240 violation. Reliability*First* determined that URE did not revoke the physical access of three employees who transferred to positions that did not require such access to CCAs, within seven calendar days.

CIP-006-1 R1.2 - OVERVIEW

URE submitted a Self-Report to Reliability*First* identifying this violation. Reliability*First* determined that URE had an unidentified access point to a PSP and measures to control those access points in its physical security plan.

CIP-006-1 R3 - OVERVIEW

URE submitted a Self-Report to Reliability*First* identifying this violation. Reliability*First* determined that URE failed to monitor continuously a workstation and a cabinet that are PSPs that house CCAs and did not implement the technical and procedural controls for monitoring physical access at all access points to those two PSPs 24 hours a day, seven days a week.

CIP-006-1 R1.8 and CIP-006-2 R2.2 - OVERVIEW

URE submitted a Self-Report to Reliability*First* identifying this violation. Reliability*First* determined that URE did not afford the protections of CIP-004-1 R3/CIP-004-2 R3 to its building access system, a cyber asset used in the access control and monitoring of the PSP. There was one protective measure set forth in CIP-004 R3 which was not afforded the building access system used in the access control and monitoring of the PSP, that of obtaining PRAs for this group of seven employees.

CIP-007-1 and CIP-007-2a R6 - OVERVIEW

URE submitted a Self-Report to Reliability*First* identifying this violation. Reliability*First* determined that URE did not produce and retain for 90 calendar days all logs for two Critical Cyber Assets as specified in R6.

CIP-006-2c R4- OVERVIEW

URE submitted this violation as one of three Self-Reports for violations arising from the loss of electrical power after an electrical fire in a generating complex. Reliability*First* determined that URE did not implement its operational and procedural controls to manage physical access at all access points to the PSPs 24 hours a day, seven days a week because the fire and power outages resulted in the card readers not communicating properly with the corporate security computer.

CIP-006-2c R5- OVERVIEW

URE submitted this violation as one of three Self-Reports for violations arising from the loss of electrical power after an electrical fire in a generating complex. Reliability*First* determined that URE did not implement its technical and procedural controls for monitoring physical access at all access points to the PSPs 24 hours a day, seven days a week.

CIP-006-2c R6- OVERVIEW

URE submitted this violation as one of three Self-Reports for violations arising from the loss of electrical power after an electrical fire in a generating complex. Reliability*First* determined that URE as a result of the fire causing the power outages and prior to the security officers being stationed at the access points, did not implement its technical and procedural mechanisms for logging physical entry at all access points to the PSPs, thereby failing to implement logging that records sufficient information to uniquely identify individuals and the time of access 24 hours a day, seven days a week.

CIP-006-3c R4- OVERVIEW

URE submitted this violation as one of three Self-Reports for violations arising from URE granting physical access to a room containing CCAs to two contractors when the individual escorting the contractors was not present with the contractors at all times. The contractors had unauthorized unescorted physical access to the room with the CCAs from 10:07 a.m. EST until 4:49 p.m. EST on October 19, 2010 and from 7:08 a.m. EST until 4:11 p.m. EST on October 2010. Reliability*First* determined that URE did not implement its operational and procedural controls to manage physical access at all access points to the PSP 24 hours a day, seven days a week.

CIP-006-3c R5- OVERVIEW

URE submitted this violation as one of three Self-Reports for violations arising from URE granting physical access to a room containing CCAs to two contractors when the individual escorting the contractors was not present with the contractors at all times. Reliability*First* determined that URE did not implement its technical and procedural controls for monitoring physical access at all access points to the PSP 24 hours a day, seven days a week.

CIP-006-3c R6- OVERVIEW

URE submitted this violation as one of three Self-Reports for violations arising from URE granting physical access to a room containing CCAs to two contractors when the individual escorting the contractors was not present with the contractors at all times. Reliability*First* determined that URE did not implement the technical and procedural mechanisms for logging physical entry at all access points to the PSP, thereby failing to record sufficient information to uniquely identify individuals and the time of access 24 hours a day, seven days a week.

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

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines, the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[11] 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 an eighty-five thousand dollar ($85,000) 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. Reliability*First* considers the instant violations of CIP-006-1 R1.8; CIP-006-2c R4, R5, and R6; and CIP-006-3c R4, R5, and R6 as repetitive conduct which was an aggravating factor in penalty determination;[12]
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

[10] *See* 18 C.F.R. § 39.7(d)(4).

[11] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

[12] The conduct of the CIP-006 violations is similar to that underlying the prior violations of the same and closely-related Reliability Standard Requirements. Reliability*First* has concluded that all of the alleged violations of CIP-006 implicate that URE has repeatedly failed to ensure the physical security of its CCAs.

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 eighty-five thousand dollars ($85,000) 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.

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 February 24, 2011, included as Attachment a;

   i. URE' Self-Report for CIP-006-2c R4, included as Attachment A to the Settlement Agreement;

   ii. URE' Mitigation Plan for CIP-006-2c R4, R5, and R6, included as Attachment B to the Settlement Agreement;

   iii. URE' Certification of Mitigation Plan Completion for CIP-006-2c R4, R5, and R6, included as Attachment C to the Settlement Agreement;

   iv. URE' Self-Report for CIP-006-2c R5, included as Attachment D to the Settlement Agreement;

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

v. URE' Self-Report for CIP-006-2c R6, included as Attachment E to the Settlement Agreement;

vi. URE' Self-Report for CIP-006-3c R4, included as Attachment F to the Settlement Agreement;

vii. URE' Mitigation Plan for CIP-006-3c R4, R5, and R6, included as Attachment G to the Settlement Agreement;

viii. URE' Certification of Mitigation Plan Completion for CIP-006-3c R4, R5, and R6, included as Attachment H to the Settlement Agreement;

ix. URE' Self-Report for CIP-006-3c R5, included as Attachment I to the Settlement Agreement;

x. URE' Self-Report for CIP-006-3c R6, included as Attachment J to the Settlement Agreement;

xi. URE' Self-Report for CIP-004-1 R4.2, included as Attachment K to the Settlement Agreement;

xii. URE' Mitigation Plan for CIP-004-1 R4.2, included as Attachment L to the Settlement Agreement;

xiii. URE' Certification of Mitigation Plan Completion for CIP-004-1 R4.2, included as Attachment M to the Settlement Agreement;

xiv. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R4.2, included as Attachment N to the Settlement Agreement;

xv. URE' Self-Report for CIP-004-1 R4.2, included as Attachment O to the Settlement Agreement;

xvi. URE' Mitigation Plan for CIP-004-1 R4.2, included as Attachment P to the Settlement Agreement;

xvii. URE' Certification of Mitigation Plan Completion for CIP-004-1 R4.2, included as Attachment Q to the Settlement Agreement;

xviii. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R4.2, included as Attachment R to the Settlement Agreement;

xix. URE' Self-Report for CIP-006-1 R1.2, included as Attachment S to the Settlement Agreement;

xx. URE' Mitigation Plan for CIP-006-1 R1.2, included as Attachment T to the Settlement Agreement;

xxi. URE' Certification of Mitigation Plan Completion for CIP-006-1 R1.2, included as Attachment U to the Settlement Agreement;

xxii. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-1 R1.2, included as Attachment V to the Settlement Agreement;

xxiii. URE' Self-Report for CIP-006-1 R3, included as Attachment W to the Settlement Agreement;

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

xxiv. URE' Mitigation Plan for CIP-006-1 R3 s, included as Attachment X to the Settlement Agreement;

xxv. URE' Certification of Mitigation Plan Completion for CIP-006-1 R3, included as Attachment Y to the Settlement Agreement;

xxvi. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-1 R3, included as Attachment Z to the Settlement Agreement;

xxvii. URE' Self-Report for CIP-006-1 R1.8 and CIP-006-2 R2.2, included as Attachment AA to the Settlement Agreement;

xxviii. URE' Mitigation Plan for CIP-006-1 R1.8 and CIP-006-2 R2.2, included as Attachment BB to the Settlement Agreement;

xxix. URE' Certification of Mitigation Plan Completion for CIP-006-1 R1.8 and CIP-006-2 R2.2, included as Attachment CC to the Settlement Agreement;

xxx. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-1 R1.8 and CIP-006-2 R2.2, included as Attachment DD to the Settlement Agreement;

xxxi. URE' Self-Report for CIP-007-1 and CIP-007-2a R6, included as Attachment EE to the Settlement Agreement;

xxxii. URE' Mitigation Plan for CIP-007-1 and CIP-007-2a R6 , included as Attachment FF to the Settlement Agreement;

xxxiii. URE' Certification of Mitigation Plan Completion for CIP-007-1 and CIP-007-2a R6, included as Attachment GG to the Settlement Agreement;

xxxiv. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 and CIP-007-2a R6, included as Attachment HH to the Settlement Agreement;

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

i. Disposition Document for CIP-004-1 R4.2 (2 occurrences), included as Attachment b.1;

ii. Disposition Document for CIP-006 violations, included as Attachment b.2;

iii. Disposition Document for CIP-007 violations, included as Attachment b.3.

c) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-2c R4, R5, and R6, included as Attachment c; and

d) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-3c R4, R5, and R6, included as Attachment d.

A Form of Notice Suitable for Publication[13]

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

[13] *See* 18 C.F.R. § 39.7(d)(6).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net Amanda E. Fried* Associate Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 amanda.fried@rfirst.org	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 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 Megan E. Gambrel* Associate Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 megan.gambrel@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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
Sonia C. Mendonça
Attorney North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment b

Disposition Document for Common Information

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

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS
Dated June 10, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-820**

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 **$85,000** FOR **TWELVE** 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
Reliability*First* noted that URE's instant violation of CIP-006-1 R1.2 constitutes the first instance of URE's violation of CIP-006. In light of that violation, Reliability*First* considers the instant violations of CIP-

[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.

006-1 R1.8, CIP-006-2c R4, R5, and R6, and CIP-006-3c R4, R5, and R6 as repetitive conduct because the conduct is similar to that underlying the prior violations of the same and closely-related Reliability Standard Requirements. Reliability*First* has concluded that all of the violations of CIP-006 implicate that URE has repeatedly failed to ensure the physical security of its CCAs and therefore considered this repetitive conduct as an aggravating factor in the penalty determination.

Reliability*First* did not consider the second instance of CIP-004-1 R4.2 (RFC201000240) to be a second violation because it occurred concurrently to and was discovered while URE was investigating and performing mitigating actions for CIP-004-1 R4.2 (RFC201000234).

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

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

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ NO ☐ UNDETERMINED ☐
EXPLAIN
URE had a compliance program in place at the time of the violations. Reliability*First* considered certain aspects of URE' compliance program as mitigating factors when 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

(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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

OTHER RELEVANT INFORMATION:

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

SETTLEMENT REQUEST DATE
DATE: **2/22/11** 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 R4.2 (2 occurrences)

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

DISPOSITION OF VIOLATION
Dated June 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000234 (1st instance)	**RFC201000234**
RFC201000240 (2nd instance)	**RFC201000240**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**4**	**4.2**	**Medium[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 provides 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.**

****

[1] 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.

[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.

> **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.**

(Footnote added).

VIOLATION DESCRIPTION

URE submitted a Self-Report to Reliability*First* stating that two URE employees with physical access to Critical Cyber Assets (CCAs) transferred to positions that did not require physical access to CCAs on November 16, 2009, and December 2, 2009, respectively. On January 12, 2010, URE discovered that although the two employees transferred to positions no longer requiring physical access to CCAs, URE failed to revoke their access to the CCAs within seven calendar days.

After the incident that led to the self-reporting of RFC201000234, and as part of its investigation and mitigating actions, URE conducted a manual review of all employees with unauthorized physical access to CCAs. As a result of this review, URE submitted a Self-Report to Reliability*First* stating that on December 16, 2009, an employee transferred from a position requiring access to CCAs, to a location with no CCAs. URE' system erroneously denoted the employee's new position as being at the former location. Consequently, the employee remained on the access list, and URE failed to revoke the employee's access within seven calendar days.

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 prior to the violation, all three employees had completed both a PRA and CIP training because URE only grants unescorted physical access to CCAs to those employees who have both Personnel Risk Assessments (PRAs) and CIP training. In addition, all three employees transferred to new positions within the company and were still subject to the URE code of conduct and the corporate policy for Cyber Security. Finally, the three employees did not physically access nor did they have cyber access to the CCAs during the time period of the violations.

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	☐

DURATION DATE(S)

RFC201000234 (1st instance)
1/1/10[4] (when URE was subject to compliance with this standard as a "Table 3" entity) through 1/12/10 (the date URE revoked the two individuals' physical access to CCAs)

RFC201000240 (2nd instance)
1/1/10[5] (when URE was subject to compliance with this standard as a "Table 3" entity) through 1/21/10 (the date URE revoked the individual's physical access to CCAs)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

RFC201000234 (1st instance)	**Self-Report**
RFC201000240 (2nd instance)	**Self-Report**

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

[4] The violative conduct began on November 23, 2009, and December 9, 2009, the date by which URE should have revoked access for the two individuals.
[5] The violative conduct began on December 23, 2009, the date by which URE should have revoked access.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

III. MITIGATION INFORMATION

RFC201000234 (1st instance)
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2497**
DATE SUBMITTED TO REGIONAL ENTITY	**4/22/10**
DATE ACCEPTED BY REGIONAL ENTITY	**5/6/10**
DATE APPROVED BY NERC	**5/26/10**
DATE PROVIDED TO FERC	**5/26/10**

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	**1/21/10**
DATE OF CERTIFICATION LETTER	**6/9/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**1/21/10**
DATE OF VERIFICATION LETTER	**8/5/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**1/21/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE revoked CCA access to the two individuals that no longer required CCA access. Additionally, URE completed a manual review of its access list for unescorted physical access to all CCAs after determining that conducting an electronic review of the access list prior to January 1, 2010 as not possible. URE was then able to identify all individuals with authorized access to CCAs prior to January 1, 2010 who no longer required such access and revoked their access in accordance with the Standard.

Procedures were put in place to ensure employees and contractors changing job status beginning January 1, 2010, whether being reassigned, retiring or terminated for cause, are evaluated to determine if their unescorted physical or authorized cyber access to CCAs needs to be terminated. For additional awareness, a CIP Senior Manager distributed a letter to all generation supervisors and employees associated with CCAs, emphasizing the importance of communicating promptly changes in employee job status, including reassignment, retirement and termination for cause.

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 procedure document that is used for authorizing and documenting who has physical and/or electronic access to CCAs.**
- **Incident Report stating that, Corporate Security ran a CIP Perimeter Security Perimeter Access Investigation Report.**

RFC201000240 (2nd instance)
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2498**
DATE SUBMITTED TO REGIONAL ENTITY	**4/22/10**[6]
DATE ACCEPTED BY REGIONAL ENTITY	**5/6/10**[7]
DATE APPROVED BY NERC	**5/26/10**
DATE PROVIDED TO FERC	**5/26/10**

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	**1/21/10**
DATE OF CERTIFICATION LETTER	**6/9/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**1/21/10**
DATE OF VERIFICATION LETTER	**8/5/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**1/21/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
A Corporate Security administrator deleted the access code from the employee's ID badge on January 21, 2010 at 7:30 a.m. Corporate Security also ran an activity report on the employee and it was determined that the ID badge was not used to gain access to any Physical Security Perimeter. URE' actions it took to address the prior violation of CIP-004-1 R4.2 memorialized in the Mitigation Plan MIT-10-2497 for RFC201000234 also mitigated this violation.

[6] The Mitigation Plan was signed on April 21, 2010.
[7] The Verification of Mitigation Plan Completion incorrectly states that Reliability*First* accepted the Mitigation Plan on April 23, 2010.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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 procedure that is used for authorizing and documenting who has physical and/or electronic access to CCAs.**
- **Incident Report stating that, Corporate Security ran a CIP Perimeter Security Perimeter Access Investigation Report.**

EXHIBITS:

SOURCE DOCUMENT
URE' Self-Report for CIP-004-1 R4.2 RFC201000234 URE' Self-Report for CIP-004-1 R4.2 RFC201000240

MITIGATION PLAN
URE' Mitigation Plan MIT-10-2497 for CIP-004-1 R4.2
URE' Mitigation Plan MIT-10-2498 for CIP-004-1 R4.2

CERTIFICATION BY REGISTERED ENTITY
URE' Certification of Mitigation Plan Completion for CIP-004-1 R4.2 RFC201000234
URE' Certification of Mitigation Plan Completion for CIP-004-1 R4.2 RFC201000240

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R4.2 RFC201000234
Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R4.2 RFC201000240

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-006 violations

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

DISPOSITION OF VIOLATION
Dated June 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000241	**RFC201000241**
RFC201000295	**RFC201000295**
RFC201000432	**RFC201000432**
RFC201000658	**RFC201000658**
RFC201000659	**RFC201000659**
RFC201000660	**RFC201000660**
RFC201000681	**300735**
RFC201000682	**300736**
RFC201000683	**300737**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-006-1	**1**	**1.2**	**Medium**[1]	**N/A**[2]
CIP-006-1	**3**		**Medium**[3]	**N/A**
CIP-006-1/ CIP-006-2[4]	**1/ 2**	**1.8/ 2.2**	**Lower**[5]	**N/A Lower**[6]
CIP-006-2c	**4**		**Medium**	**High**
CIP-006-2c	**5**		**Medium**	**High**
CIP-006-2c	**6**		**Lower**	**High**
CIP-006-3c	**4**		**Medium**	**Moderate**[7]

[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, R1.8 and R1.9 each have a "Lower" VRF.
[2] At the time of URE' violations of CIP-006-1 R1 and CIP-006-1 R3, no 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. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards; the Commission approved the VSLs on March 18, 2010.
[3] CIP-006-1 R3, R3.1 and R3.2 each have a "Medium" VRF and R3.3 has a "Lower" VRF.
[4] CIP-006-1 became effective on January 1, 2010 for "Table 3" entities and was superseded by CIP-006-2 on April 1, 2010. URE' violation included instances that occurred both before and after April 1, 2010. When CIP-006-2 became effective, the "Cyber Assets used in the access control and monitoring of the Physical Security Perimeter" from CIP-006-1 R1.8 became "Cyber Assets that authorize and/or log access to the Physical Security Perimeter" in CIP-006-2 R2. The Settlement Agreement uses the terminology from CIP-006-1 R1.8 throughout, and where applicable, designates the language from CIP-006-2 R2.2.
[5] The VRF for CIP-006-2 R2.2 is "Medium" which became effective on April 1, 2010.
[6] On December 18, 2009, NERC submitted revised VRFs and VSLs for CIP-002-2 through CIP-009-2. On January 20, 2011, FERC issued an order approving the Version 2 VRFs and VSLs and made them effective on April 1, 2010, the date the Version 2 CIP Reliability Standards became effective.

CIP-006-3c	**5**		**Medium**	**Moderate**
CIP-006-3c	**6**		**Medium**	**Moderate**

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: "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…."[8]

CIP-006-1 R1 and R3 provides in pertinent part:

> **R1. Physical Security Plan — The Responsible Entity[9] shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:**
>
> ***
>
> **R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.**
>
> ***
>
> **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[10] Requirement R3, Standard CIP-005 Requirements**

---

[7] On December 29, 2009, NERC submitted revised VRFs and VSLs for CIP-002-3 through CIP-009-3. On January 20, 2011, FERC issued an order approving the Version 3 VRFs and VSLs and made them effective on October 1, 2010, the date the Version 3 CIP Reliability Standards became effective.

[8] The Purpose statement was not altered between versions CIP-006-1, CIP-006-2c, and CIP-006-3c.

[9] 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.

[10] CIP-006-2 R2.2 uses the language: "Standard CIP-004-2 Requirement R3." Standard CIP-004-2 R3 requires entities to have a documented PRA program for personnel who have authorized cyber or authorized unescorted physical access to CCAs.

> **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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:

> **R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.**
>
> ***
>
> **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 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.**

(Footnotes added)

CIP-006-2c and CIP-006-3c provide in pertinent part:[11]

> **R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:**

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

[11] This section uses the terminology from CIP-006-3c, and where applicable, designates the language from CIP-006-2c.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

• Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

• Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. 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 access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3.[12] One or more of the following monitoring methods shall be used:

• 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.

• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

[12] CIP-006-2c uses the language: "…specified in Requirement CIP-008-2".

• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

• Video Recording: Electronic capture of video images of sufficient quality to determine identity.

• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

(Footnote added)

VIOLATION DESCRIPTION

RFC201000241 – CIP-006-1 R1.2
URE submitted a Self-Report to Reliability*First* stating that it had failed to identify an access point to the Physical Security Perimeter (PSP) for a Control Room (Control Room) in its physical security plan. In 2010, URE completed a site assessment of the Control Room, which is within a PSP, and located an unidentified access point to the PSP from the roof of the Control Room where there are three potential means of access.

RFC201000295 – CIP-006-1 R3
URE submitted a Self-Report to Reliability*First* identifying that its breaker house for two units contains a workstation and a cabinet that are PSPs that house Critical Cyber Assets (CCAs). URE failed to monitor continuously both the workstation and the cabinet, though they were both locked and had controlled keys. When URE discovered the issue, it attempted to install card readers on the workstation and cabinet to provide continuous monitoring but encountered difficulties during installation and learned the readers did not provide continuous monitoring. URE then posted security officers to monitor the workstation and cabinet until security cameras were installed.

RFC201000432 – CIP-006-1 R1.8/ CIP-006-2 R2.2
URE submitted a Self-Report to Reliability*First* identifying seven individuals with access to certain cyber assets that did not have complete or current Personnel Risk Assessments (PRAs) in accordance with the Standard. The seven individuals, all of which are database administrators, had access to data related to URE' building access system, which is a designated Cyber Asset. The building access system provides access control and monitoring of URE' PSPs by restricting access to the PSPs to authorized employees and contractors, and logging authorized and attempted unauthorized access. As a result, URE is required to afford this building access system the protections set forth in CIP-004 R3. There was one protective measure set forth in CIP-004 R3 which was not afforded the building access system

used in the access control and monitoring of the PSP, that of obtaining PRAs for this group of seven employees.

CIP-006-2c R4, R5, R6
One of URE's buildings experienced an electrical fire. URE subsequently disconnected electrical power to the building, resulting in the deenergizing of a second URE building and the security system communication module service in a third building. In an attempt to fight the fire, URE removed power from the first building. The breaker that electrically feeds the first building also feeds the second building and site annex. These power outages affected five PSPs, two in the first building, one in the third building, and two in the second building. The violations of CIP-006-2c R4, R5, and R6 discussed below are related to the power outages.

URE submitted a Self-Report to Reliability*First* reporting these three violations.

RFC201000658 – CIP-006-2c R4
In the October 13, 2010 Self-Report, URE stated that as a result of the fire causing the power outages, the access control card readers (card readers) for five access points (one into each of the five PSPs affected by the fire) provided access to anyone with a URE identification badge. The corporate security computer system grants access based on individual credentials, but the fire and power outages resulted in the card readers not communicating properly with the corporate security computer. The card readers were unable to differentiate among access levels. After 16 hours and 20 minutes, when URE determined the card readers were not functioning correctly, it stationed security officers at the access points until the card readers were operational. The security officers did not have the ability to validate authorization levels, but they did maintain accurate logs and visually monitored all entrants to the access points to the PSPs.

RFC201000659 – CIP-006-2c R5
In the Self-Report, URE stated that as a result of the fire causing the power outages and prior to the security officers being stationed at the access points, the card readers failed to generate an alarm when an unauthorized access attempt occurred or when a door was forced or held open. The card readers at each of the five access points could not communicate with the corporate security computer system which normally generates alarms to the personnel responsible for response.

RFC201000660 – CIP-006-2c R6
In the Self-Report, URE stated that as a result of the fire causing the power outages and prior to the security officers being stationed at the access points, the card readers at each of the five access points could not communicate with the corporate security computer system and therefore did not capture access logs with sufficient information to uniquely identify individuals and the time of access 24 hours a day, seven days a week.

CIP-006-3c R4, R5, and R6
URE has a documented physical security control policy, pursuant to CIP-006-3c, which requires an escort to provide physical access control to individuals without unescorted physical access to PSPs. On two consecutive days, URE granted physical access to a room at the Control Center of two units containing CCAs to two contractors. The contractors had unauthorized unescorted physical access to the room with the CCAs from 10:07 a.m. EST until 4:49 p.m. EST on October 19, 2010 and from 7:08 a.m. EST until 4:11 p.m. EST on October 20, 2010. The individual escorting the contractors was not present with the contractors at all times due to the escort not clearly understanding an escort's responsibilities. The violations of CIP-006-3c R4, R5, and R6 discussed below are related to these two contractors' access to the room containing CCAs.

URE submitted a Self-Report to Reliability*First* reporting these three violations.

RFC201000681 – CIP-006-3c R4
In the Self-Report, URE stated that the project for which the contractors had access required the disarming of a CCA door. The individual escorting the contractors was not present with the contractors at all times, and therefore URE failed to manage physical access control to the PSP.

RFC201000682 – CIP-006-3c R5
In the Self-Report, URE stated that the contractors were running tubing into the room through the open door, which, if enabled, would trigger an alarm. From 1:05 p.m. EST until 4:49 p.m. EST on October 19, and from 7:26 a.m. EST until 7:57 a.m. EST on October 20, URE disabled the alarm system for monitoring physical access in order to perform routine maintenance on the building, and the escort required to monitor physical access while the alarm system was disabled was not present.

RFC201000683 – CIP-006-3c R6
In the Self-Report, URE stated that it failed to log the time of the contractors' access to the PSP, as required by its physical security control policy, because the two contractors did not log in and out as required.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL
CIP-006-1 R1.2
Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because each of the three potential means of access to the unidentified roof access point is unlikely to be accessed. First, in the Control Room, the rolling platform is typically stored approximately 20 feet below the entry point, and the roof is approximately 30 feet from the ground. Second, the building's elevator control room remains locked at all times, and the only keys are located with the elevator repair company and with the electrical group, which is comprised of the two units' electrical maintenance

supervisor and electricians who all have PRAs and have successfully completed required training. Finally, utilizing external means, such as a ladder, to gain access to the roof, which is approximately 30 feet from the ground, is unlikely. There is also no evidence of unauthorized physical entry or physical or cyber tampering to the Control Room during the relevant time period.

CIP-006-1 R3
Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the BPS because URE kept both the cabinet and the workstation locked, and implemented constant key logging. URE reviewed these paper logs and based on that review, there was no evidence of unauthorized access to either the workstation or the cabinet at any time.

CIP-006-1 R1.8/ CIP-006-2 R2.2
Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the BPS because although the building access system is a cyber asset used in the access control and monitoring of the PSP, it is separate from the networks that support the bulk electric system. This mitigated the risk of an individual with access to the building access system but without the requisite PRA from being able to affect the BPS. In addition, after conducting the PRAs for the seven individuals, there were no identified issues. There is also no evidence of inappropriate or direct changes made to the building access data during the relevant period, demonstrating that the individuals without complete PRAs did not tamper with the building access data.

CIP-006-2c R4, R5, R6
Reliability*First* determined that the violations did not pose a serious or substantial risk to the reliability of the BPS because one of the units was not operational at the time of the fire. Since the Unit was not operational, unauthorized access to this unit was less likely to affect the reliability of the BPS. Additionally, the fire did not affect second unit, so it continued to operate successfully. The card readers affected do not protect any CCAs of the second unit, so there was no risk of unauthorized access to it. Once URE determined both that the card readers and their associated logging and alarms were not functional and that the situation was safe, URE stationed security officers at all the access points until it restored power.

CIP-006-3c R4, R5, R6
Reliability*First* determined that the violations did not pose a serious or substantial risk to the reliability of the BPS because the room at issue contains CCAs that control only the two units, and the second unit was not operating at the time of the event because it was undergoing a periodic maintenance outage. In addition, the companies providing contracted services in this instance have had a successful long-standing relationship with URE.

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	☐

DURATION DATE(S)

CIP-006-1 R1.2
1/1/10 (when URE was subject to compliance with the standard as a "Table 3" entity) through 1/22/10 (when URE bolted the roof entry point from the inside to preclude access)

CIP-006-1 R3
1/1/10 (when URE was subject to compliance with the standard as a "Table 3" entity) through 3/5/10 (when URE placed a security officer in the breaker house to provide continuous monitoring of the workstation and the cabinet)

CIP-006-1 R1.8/ CIP-006-2 R2.2
1/31/10 (when URE granted the unauthorized access) through 6/29/10 (when URE completed current PRAs for the seven individuals)
CIP-006-2c R4
9/15/10 at 3:08 p.m. EST (the time of the outage) through 9/17/10 at 2:08 p.m. EST (when URE restored temporary power to the security equipment)

CIP-006-2c R5
9/15/10 at 3:08 p.m. EST (the time of the outage) through 9/17/10 at 7:28 a.m. EST (when URE posted security officers at the access points)

CIP-006-2c R6
9/15/10 at 3:08 p.m. EST (the time of the outage) through 9/17/10 at 7:28 a.m. EST (when URE posted security officers at the access points)

CIP-006-3c R4, R5, R6
10/19/10 (when the two contractors first gained access to the room containing CCAs without an escort) through 10/20/10 (when the two unescorted contractors were no longer in the room)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

CIP-006-1 R1.2 **Self-Report**

CIP-006-1 R3	**Self-Report**
CIP-006-1 R1.8/ CIP-006-2 R2.2	**Self-Report**
CIP-006-2c R4, R5, R6	**Self-Report**
CIP-006-3c R4, R5, R6	**Self-Report**

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

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

III. MITIGATION INFORMATION

CIP-006-1 R1.2

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2499**
DATE SUBMITTED TO REGIONAL ENTITY	**4/22/10**[13]
DATE ACCEPTED BY REGIONAL ENTITY	**5/6/10**[14]
DATE APPROVED BY NERC	**5/26/10**
DATE PROVIDED TO FERC	**5/26/10**

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	**1/22/10**
DATE OF CERTIFICATION LETTER	**6/9/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**1/22/10**
DATE OF VERIFICATION LETTER	**7/27/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**1/22/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE secured the roof access point by bolting it from the inside and installing audible alarms. URE additionally performed a walk-down of all physical

[13] The Mitigation Plan for CIP-006-1 R1.2 was signed on April 21, 2010.
[14] The Verification of Mitigation Plan Completion incorrectly states that Reliability*First* accepted the Mitigation Plan on April 23, 2010.

security perimeters to determine whether other unidentified or unsecured access points to PSPs existed and found no such access points.

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)

- **"Attachment 1 – Photos.pdf" that shows pictures at different angles of the entry point.**
- **A redacted report of the discovery of this entry point. The report gives details of the investigation with pictures and how the violation was mitigated through the installation of locks and audible alarms that sound at the Security center.**

CIP-006-1 R3

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2501**
DATE SUBMITTED TO REGIONAL ENTITY	**4/22/10**[15]
DATE ACCEPTED BY REGIONAL ENTITY	**5/6/10**
DATE APPROVED BY NERC	**5/26/10**
DATE PROVIDED TO FERC	**5/26/10**

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

N/A

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**5/28/10**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**5/27/10**
DATE OF CERTIFICATION LETTER	**6/9/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**5/27/10**
DATE OF VERIFICATION LETTER	**7/23/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**5/27/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE placed a security officer in the breaker house to provide continuous monitoring of the workstation and the cabinet until URE was able to install a security camera. URE installed the security camera in the Breaker House of the two units, which provides a live-feed to monitors in URE's Security

[15] The Mitigation Plan for CIP-006-1 R3 was signed on April 21, 2010.

Center and in the two units' plant security. Both URE's Security Center and the two units' plant security continuously monitor the workstation and the cabinet whenever its keyboard tray is open. In addition, URE updated its physical security plan to specify that URE must install continuous monitoring equipment on CCAs, and URE installed security cameras on all key card lock cabinets.

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)

- **"Camera Evidence" that contains the floor plan of where the cabinet is located and pictures from the video camera that was installed to continuously monitor physical access of the cabinet by security personnel. The pictures show an employee accessing the cabinet from different viewpoints with time and date stamps.**
- **A log of the card reader located on the cabinet was included in this document and coincides with the date and time stamps of the pictures.**

CIP-006-1 R1.8/ CIP-006-2 R2.2
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2784**
DATE SUBMITTED TO REGIONAL ENTITY	**7/19/10**
DATE ACCEPTED BY REGIONAL ENTITY	**8/10/10**
DATE APPROVED BY NERC	**9/3/10**
DATE PROVIDED TO FERC	**9/3/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**7/31/10**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**7/30/10**
DATE OF CERTIFICATION LETTER	**11/18/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**7/30/10**
DATE OF VERIFICATION LETTER	**1/10/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**7/30/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE ensured that it had properly reflected the role of the database administrators as CIP-related, and requested PRAs for all database administrators. URE also verified that all other individuals with access to the building access system and related data had PRAs. In addition, URE enhanced its existing procedures to verify that prior to providing an individual with such access; a current PRA is on file for that individual. URE checked the audit logs and authorized change reports on its system to ensure that no unauthorized changes were made to the data. To protect against recurrence of the instant violation, URE enhanced its human resources procedures to work closely with supervisors when filling vacancies to ensure the completion of the appropriate PRA review. URE reiterated to those individuals approving access to the building access system and related data that a PRA is necessary before granting access.

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)

Attachment 1
A document that provides evidence that the database administration positions have now been flagged in the HR database as requiring a PRA for the individuals holding the DBA position. If personnel are hired or transferred into a database administration position, then HR will know that a PRA will be required.

Attachment 2

- **List of database administrations PRAs completion for employees PRA completion for Contractors**
  This document provides evidence that PRAs were conducted for the seven individuals who previously did not have PRAs. For the six company employees, redacted PRAs were provided. For the one contractor, an e-mail from the contract company documents that the PRA was conducted.

Attachment 3

- **List of individuals with system access**
- **List of individuals with data access outside the application and their corresponding PRA completion records for employees and Contractors**
  This document provides evidence that all individuals who have cyber access to the building access system or related data have a current PRA. The document consists of the name of all the individuals with such access and the associated PRA completion dates.

Attachment 4

- **Audit Review Summary**
  This document provides evidence that the database administration supervisor and the application owner authorized the three changes made by an individual without a current PRA. The document is the form, which includes a description of the proposed change, authorizations, and date completed.

Attachment 5

- **IT Security Procedure Enhancements**
  This document provides evidence of changes to the IT Security Procedures. Any individual adding users to an active directory group should see the note and not proceed until they have verified that the PRA and training for the new individual is complete.

Attachment 6

- **PRA Reminder to Supervisors and Group Owners**
  This document provides evidence of an e-mail sent to management personnel reminding them of the CIP Requirements for PRAs and Training. It points out that vendors and contractors must follow the CIP Requirements as well. The e-mail provides an overview of the requirements and the procedures to be followed to ensure compliance.

Attachment 7

- **Revised HR procedures**
  This document provides evidence of changes to existing HR procedures to cover new hires, transfers, and separations. In each case, the procedures are checklists of what is required by HR and the individual's manager. The checklists cover the determination of the need for a PRA and the granting of access to critical cyber assets. It also covers the revoking of such access in the event of transfers or separation.

CIP-006-2c R4, R5, R6

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-3192**
DATE SUBMITTED TO REGIONAL ENTITY	**12/2/10**
DATE ACCEPTED BY REGIONAL ENTITY	**12/16/10**
DATE APPROVED BY NERC	**12/30/10**
DATE PROVIDED TO FERC	**1/5/11**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**1/31/11**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**2/18/11**

DATE OF CERTIFICATION LETTER	**1/31/11**[16]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**2/18/11**

DATE OF VERIFICATION LETTER	**3/2/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**2/18/11**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

Once it was identified that the five access points had lost power and monitoring was no longer being performed within the Security Center, security officers were posted at those locations to ensure all Personnel logged access using the paper logs within the PSP. URE programmed an email notification to the Security Center to supplement the alarm indicating a power failure. It changed the site setting in the access control system to maintain alarms until communications had been restored. The Critical Cyber Security System Owner(s) created a procedure for removing power to PSPs for scheduled and emergency outages. URE provided backup power to the fiber communication links to the Corporate Security Access Control Server. Finally, URE modified Corporate Security's orders and procedures such that any time a security officer needs to be posted at any access point, a list can be provided to the security officer indicating all personnel who have unescorted access to that PSP.

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)

- **"Attachment A" Screen print of e-mail notification**
- **"Attachment B" "alarm expiration threshold setting change**
- **"Attachment C" Job Aid for Removal of Power to PSPs**
- **"Attachment D" Work Order**
- **Work Order Invoice**
- **Attestation document regarding plan monitoring**

[16] On January 31, 2011, URE submitted to Reliability*First* a certification of completion for this Mitigation Plan, stating that it was complete as of January 27, 2011. On February 22, 2011, URE notified Reliability*First* that it actually completed this Mitigation Plan on February 18, 2011. URE did not submit another Certification of Mitigation Plan completion, instead URE attested to the completion of the Mitigation Plan on the later date.

- **"Attachment E" Modified orders and procedures**

RFC201000681 – CIP-006-3c R4, R5, R6

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-3418**
DATE SUBMITTED TO REGIONAL ENTITY	**1/31/11**
DATE ACCEPTED BY REGIONAL ENTITY	**2/15/11**
DATE APPROVED BY NERC	**3/16/11**
DATE PROVIDED TO FERC	**3/17/11**

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	**1/14/11**
DATE OF CERTIFICATION LETTER	**1/31/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**1/14/11**
DATE OF VERIFICATION LETTER	**3/24/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**1/14/11**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
Upon learning of the issue, URE removed unescorted access privileges of the responsible individuals. In addition, all those who were responsible, including contractors, were coached and counseled on appropriate procedures. The lead met with the Engineering department's Project Managers and reviewed the policy, site expectations, and personal responsibilities, in regard to the NERC CIP physical security plan. The procedure for disarming a CCA door was revised and communicated with additional measures to be taken in the even such a door must be disarmed. The measures include the mandatory dispatch of a security officer as an escort. On November 1, 2010 and January 14, 2011, a communication event was held to reinforce adherence to existing policies.

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)

- **"Attachment A" Procedure re: Request to Block Door Open**
- **"Attachment B" 11-1-10 Presentation on CIP Physical Security Requirements**
- **"Attachment C" 11-1-10 Attendance Sheet**
- **"Attachment D" 1-14-11 Presentation on CIP Physical Access Procedures**
- **"Attachment E" 1-14-11 Attendance Sheet**

EXHIBITS:

SOURCE DOCUMENTS

URE' Self-Report for CIP-006-1 R1.2

URE' Self-Report for CIP-006-1 R3

URE' Self-Report for CIP-006-1 R1.8 and CIP-006-2 R2.2 URE' Self-Report for CIP-006-2c R4 URE' Self-Report for CIP-006-2c R5 URE' Self-Report for CIP-006-2c R6URE' Self-Report for CIP-006-3c R4 URE' Self-Report for CIP-006-3c R5 URE' Self-Report for CIP-006-3c R6

MITIGATION PLAN

URE' Mitigation Plan for CIP-006-1 R1.2URE' Mitigation Plan for CIP-006-1 R3 URE' Mitigation Plan for CIP-006-1 R1.8 and CIP-006-2 R2.2 URE' Mitigation Plan for CIP-006-2c R4, R5, and R6

URE' Mitigation Plan for CIP-006-3c R4, R5, and R6

CERTIFICATION BY REGISTERED ENTITY

URE' Certification of Mitigation Plan Completion for CIP-006-1 R1.2

URE' Certification of Mitigation Plan Completion for CIP-006-1 R3 s

URE' Certification of Mitigation Plan Completion for CIP-006-1 R1.8 and CIP-006-2 R2.2

URE' Certification of Mitigation Plan Completion for CIP-006-2c R4, R5, and R6 s

URE' Certification of Mitigation Plan Completion for CIP-006-3c R4, R5, and R6

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

VERIFICATION BY REGIONAL ENTITY

Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-1 R1.2

Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-1 R3

Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-1 R1.8 and CIP-006-2 R2.2

Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-2c R4, R5, and R6 d

Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-3c R4, R5, and R6

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007 violations

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

DISPOSITION OF VIOLATION
Dated June 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000435	**RFC201000435**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1/ CIP-007-2a[1]	**6**	**6.4**	**Lower**	**N/A[2]/ High[3]**

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

The purpose statement of CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities[4] to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…." Footnote added.[5]

CIP-007-1 R6 provides in pertinent part:

> **R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational**

[1] URE violated the standard from February 15, 2010 to September 17, 2010. CIP-007-1 became effective on January 1, 2010, which was superseded by CIP-007-2 on April 1, 2010. All relevant portions of CIP-007-2a R6 are exactly the same as CIP-007-1 R6.
[2] At the time of the violations, no VSLs were in effect for CIP-007-1. 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] On December 18, 2009, NERC submitted revised VRFs and VSLs for CIP-002-2 through CIP-009-2. On January 20, 2011, FERC issued an order approving the Version 2 VRFs and VSLs and made them effective on April 1, 2010, the date the Version 2 CIP Reliability Standards became effective.
[4] Within the text of Standard CIP-007, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.
[5] The purpose statement of CIP-007-1 has the same language of CIP-007-1 except for the following, "…as well as the other (non-critical) Cyber Assets…."

process controls to monitor system events that are related to cyber security.

****

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

VIOLATION DESCRIPTION

URE submitted a Self-Report to Reliability*First* which identified two Critical Cyber Assets (CCAs)[6] that did not produce and store all logs required by the standard for 90 calendar days. The two Cyber Assets within the ESP were the anti-virus and malicious software server and the database server for a DCS Control System (collectively, the Servers).

URE changed the administrator passwords for an appliance, which is the storage site for the logs required by CIP-007-1 R6.4 and CIP-007-2a R6. This password change inadvertently rendered the events logs on the Servers' systems inaccessible. The administrator password change inadvertently corrupted/altered the administrator's credentials and resulted in the Microsoft Windows Event Logs being inaccessible. This resulted in data gaps, including the loss of the logs required by CIP-007-1 R6 before the expiration of 90 calendar days.

Despite the foregoing events, three of the four events logs on the anti-virus and malicious software server were locally cached,[7] so all events dating back to February 15, 2010 were available. One of the logs was only available dating back to June 20, 2010, which constituted a violative data gap, wherein URE was unable to review events logs for system events. Two of the five event logs monitored on the database server for a DCS Control System were fully locally cached, causing data gaps for the three remaining event logs.

In summary, there were a total of four data gaps of the event logs, respectively: (1) February 15, 2010 through June 19, 2010 for the events log on the anti-virus and malicious software server; (2) February 15, 2010 through May 10, 2010 for one of the event logs on the database server for a DCS Control System; (3) February 15, 2010 through March 22, 2010 for the second event log on the database server for a DCS Control System; and (4) February 15, 2010 through May 28, 2010 for the third event log on the database server for a DCS Control System.

[6] These assets are cyber assets that reside within the ESP but were categorized as CCAs on URE's Critical Cyber Asset list per CIP-002-1 R4.

[7] When information is locally cached, it is stored on the system. Thus, the system stored the events logs before the password change, and the logs remained there.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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 both of the Servers accurately captured the event logs before the password change and so immediately prior to and subsequent to the gap, there are logs. After URE discovered the issue, it immediately attempted to restore the event logging capability. In addition, URE reviewed all fully cached logs for security events and found no cyber incidents. Importantly, URE implemented and completed these activities within four hours of discovering the issue.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) **2/15/10 (when URE changed the administrator passwords) through 9/17/10 (90 days after the date URE again retained the required logs)**

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2806**
DATE SUBMITTED TO REGIONAL ENTITY	**8/19/10**[8]
DATE ACCEPTED BY REGIONAL ENTITY	**9/2/10**
DATE APPROVED BY NERC	**9/8/10**
DATE PROVIDED TO FERC	**9/8/10**

[8] The Mitigation Plan was signed on August 18, 2010.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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	**1/28/11**[9]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**7/30/11**
DATE OF VERIFICATION LETTER	**2/11/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**7/30/11**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE revised the procedure for changing administrative passwords to include a connectivity test, which will ensure that the Cyber Assets continue functioning after a password change. In addition, URE included a weekly verification of all communications between CCAs and the appliance to ensure that the events are being logged properly.

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 URE revised the procedure for changing passwords. Step 4 of the procedure now requires the employee to verify that all devices are still in communication with the servers immediately following the change of the password. This step was added to prevent a recurrence of this type of violation.

A document that provides evidence that URE changed the procedure for verifying the monitoring of system events. Step 5 has been added to require an employee to review the Failed Logon Report and Password Event Report on a weekly basis to verify that the servers have had no issues logging into the devices in order to retrieve the system event information. URE added this step to catch the login problem before it leads to another similar violation.

[9] The Certification of Mitigation Plan Completion was signed on January 17, 2011.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

EXHIBITS:

SOURCE DOCUMENT
URE Self-Report for CIP-007-1/CIP-007-2a R6, R6.4
MITIGATION PLAN
URE Mitigation Plan MIT-10-2906

CERTIFICATION BY REGISTERED ENTITY
URE Certification of Mitigation Plan Completion

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 and CIP-007-2a R6