PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 28, 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 Entities
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 1 (URE 1), Unidentified Registered Entity 3 (URE 3), and Unidentified Registered Entity 3 (URE 2), (Collectively, the UREs), 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 the UREs have entered into a Settlement Agreement to resolve all outstanding issues arising from Reliability*First*'s determination and findings of the violations of CIP-005-1, Requirement (R) 2; CIP-005-1 R3; CIP-006-1 R1.1; CIP-007-1 R 6; CIP-004-2 R2.1; CIP-004-1 R4.2; CIP-005-1 R1; CIP-006-2 R1; CIP-007-2a R1; CIP-007-2 R3.1; CIP-007-2 R5.2.3; CIP-004-2 R2; CIP-004-2 R3; CIP-004-2 R4; and CIP-004-3 R3. According to the Settlement Agreement, the UREs agree and stipulate to the Settlement Agreement in its entirety and neither admit nor deny that the facts stipulated in the Settlement Agreement constitute

[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

violations, and have agreed to the assessed penalty of one hundred eighty thousand dollars ($180,000), 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 RFC201000226; RFC201000227; RFC201000228; RFC201000229; RFC201000230; RFC201000231; RFC201000424; RFC201000425; RFC201000594; RFC201000595; RFC201000596; RFC201000597; RFC201000598; RFC201000599; RFC201000600; RFC201000601; RFC201000602; RFC201000603; RFC201000604; RFC201000605; RFC201000661; RFC201100726; RFC201100727; RFC201100728; RFC201100729; RFC201100730; RFC201100731; and RFC201100732 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 April 12, 2011, by and between Reliability*First* and the UREs. 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-857	RFC201000226	CIP-005-1	2	Medium[3]	1/1/10-12/23/10	180,000
	RFC201000227	CIP-005-1	3	Medium	1/1/10-12/23/10	
	RFC201000228	CIP-006-1	1.1	Medium[4]	1/1/10-12/23/10	
	RFC201000229	CIP-005-1	2	Medium	1/1/10-12/23/10	
	RFC201000230	CIP-005-1	3	Medium	1/1/10-12/23/10	
	RFC201000231	CIP-006-1	1.1	Medium	1/1/10-12/23/10	
	RFC201000424	CIP-007-1	6	Lower[5]	1/1/10-6/18/10	
	RFC201000425	CIP-007-1	6	Lower	1/1/10-6/18/10	

[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-006 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.
[5] CIP-007-1 R6, R6.4 and R6.5 are assigned Lower VRFs and CIP-007-1 R6.1, R6.2 and R6.3 each are assigned a Medium VRF.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

	RFC201000594	CIP-004-2	2.1	Medium[6]	6/16/10-6/22/10	
	RFC201000595	CIP-004-1	4.2	Medium[7]	1/1/10-6/28/10	
	RFC201000596	CIP-005-1	1	Medium[8]	1/1/10-8/25/10	
	RFC201000597	CIP-006-2	1	Medium	6/18/10-7/21/10	
	RFC201000598	CIP-007-2a	1	Medium[9]	6/21/10-6/30/10	
	RFC201000599	CIP-007-2	3.1	Lower	1/1/10-7/14/10	
	RFC201000600	CIP-004-2	2.1	Medium	6/16/10-6/22/10	
	RFC201000601	CIP-004-1	4.2	Medium	1/1/10-6/28/10	
	RFC201000602	CIP-005-1	1	Medium	1/1/10-8/25/10	
	RFC201000603	CIP-006-2	1	Medium	6/18/10-7/21/10	
	RFC201000604	CIP-007-2a	1	Medium	6/21/10-6/30/10	
	RFC201000605	CIP-007-2	3.1	Lower	1/1/10-7/14/10	
	RFC201000661	CIP-007-2	5.2.3	Medium[10]	8/13/10-8/16/10	
	RFC201100726	CIP-004-2	2	Medium	7/20/10-7/21/10	
	RFC201100727	CIP-004-2	3	Medium[11]	7/20/10-7/21/10	
	RFC201100728	CIP-004-2	4	Medium	6/16/10-11/22/10	
	RFC201100729	CIP-004-2	2	Medium	7/20/10-7/21/10	
	RFC201100730	CIP-004-2	3	Medium	7/20/10-7/21/10	
	RFC201100731	CIP-004-2	4	Medium	6/16/10-11/22/10	
	RFC201100732	CIP-004-3	3	Medium	11/18/10-11/22/10	

[6] CIP-004 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a Lower VRF; R2.1, R2.2 and R2.2.4 each have a Medium VRF.
[7] CIP-004-1 R4 and R4.1 each have a Lower VRF; R4.2 has a Medium VRF.
[8] CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a Medium VRF; R1.6 has a Lower VRF.
[9] CIP-007 R1 and R1.1 each have a Medium VRF; R1.2 and R1.3 each have a Lower VRF.
[10] CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, R5.2.2, R5.3, R5.3.1 and R5.3.2 each have a Lower VRF; R5.1, R5.1.3, R5.2.1 and R5.2.3 each have a Medium VRF.
[11] CIP-004 R3 has a Medium VRF; R3.1, R3.2 and R3.3 each have a Lower VRF.

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

CIP-005-1 R2 (RFC201000226 and RFC201000229) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First*. Reliability*First* determined that URE 1 and URE 2 did not implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at nine electronic access points to the Electronic Security Perimeter (ESP).

CIP-005-1 R3 (RFC201000227 and RFC201000230) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First*. Reliability*First* determined that URE 1 and URE 2 did not implement a process for monitoring and logging access at access points to the ESP 24 hours a day, seven days a week.

CIP-006-1 R1.1 (RFC201000228 and RFC201000231) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First*. Reliability*First* determined that URE 1 and URE 2 did not ensure that all Cyber Assets within an ESP also reside within an identified Physical Security Perimeter (PSP).

CIP-007-1 R6 (RFC201000424 and RFC201000425) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First*. Reliability*First* determined that URE 1 and URE 2 did not configure 44 Cyber Assets located within the ESP to send log information to a centralized location to enable it to be reviewed. URE 1 and URE 2's process requires centralization in order to carry out the steps of review and retention. Therefore, URE 1 and URE 2 failed to retain logs for 90 calendar days as required by CIP-007-1 R6.4, and failed to review the logs for the existence of cyber security system events, as required by CIP-007-1 R6.5.

CIP-004-2 R2.1 (RFC201000594 and RFC201000600) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First*. Reliability*First* determined that URE 1 and URE 2 did not ensure all personnel having unescorted physical access to Critical Cyber Assets (CCAs) received the requisite training prior to granting such access on 18 occasions.

CIP-004-1 R4.2 (RFC201000595 and RFC201000601) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First*. Reliability*First* determined that URE 1 and URE 2 did not revoke the unescorted physical access rights within seven calendar days for an individual who no longer required such access.

CIP-005-1 R1 (RFC201000596 and RFC201000602) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-005-1 R1. Reliability*First* determined that URE 1 and URE 2 did not identify or document two non-critical Cyber Assets within the ESP and failed to identify and document one Cyber Asset as an access point to the ESP.

CIP-006-2 R1 (RFC201000597 and RFC201000603) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First*. Reliability*First* determined that URE 1 and URE 2 did not provide continuous escorted access of personnel not authorized for unescorted access within the PSP on two separate occasions.

CIP-007-2a R1 (RFC201000598 and RFC201000604) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-007-2a R1. Reliability*First* determined that URE 1, and URE 2 failed to ensure that a significant change to a cyber asset did not adversely affect existing cyber security controls when it installed new software onto four servers without testing whether the change would adversely affect existing cyber security controls.

CIP-007-2 R3.1 (RFC201000599 and RFC201000605) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-007-2 R3.1. Reliability*First* determined that URE 1 and URE 2, failed to assess a security-related software upgrade for URE 1 and URE 2. In addition, URE 2 miscalculated the due date for its assessment of several security patches, and assessed those security patches at 31 calendar days, one day beyond the 30 days required by the Reliability Standard.

CIP-007-2 R5.2.3 (RFC201000661) - OVERVIEW
The violation of CIP-007-2 R5.2.3 is by URE 1 only. URE 1 submitted a Self-Report to Reliability*First* identifying a violation of CIP-007-2 R5.2.3. Reliability*First* determined that URE 1 failed to implement its policy for managing the use of shared accounts when it failed to revoke an individual's access to a shared account within the seven days prescribed by the policy for revocation when access is no longer required by the individual.

CIP-004-2 R2 (RFC201100726 and RFC201100729) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First*. Reliability*First* determined that URE 1 and URE 2 failed to train an individual prior to that individual gaining unescorted access to CCAs.

CIP-004-2 R3 (RFC201100727 and RFC201100730) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First*. Reliability*First* determined that URE 1 and URE 2 failed to conduct a Personnel Risk Assessment (PRA) for the same individual as discussed in the description of RFC201100726 and RFC201100729, who had access to CCAs, prior to granting that individual access.

CIP-004-2 R4 (RFC201100728 and RFC201100731) - OVERVIEW
URE 1 and URE 2 submitted a Self-Report to Reliability*First*. Reliability*First* determined that URE 1 and URE 2 failed to revoke the unescorted physical access rights within seven calendar days for an individual who no longer required such access.

CIP-004-3 R3 (RFC201100732) - OVERVIEW
URE 3 submitted a Self-Report to Reliability*First*. Reliability*First* determined that URE 3 failed to conduct a PRA prior to an individual being granted unescorted physical access to a PSP.

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

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines, the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[13] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on July 11, 2011. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of a one hundred eighty thousand dollar ($180,000) financial penalty against the UREs and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. The UREs promptly self-reported the violations by calling Reliability*First* and verbally reporting some of the violations before submitting additional Self-Reports;
2. Reliability*First* reported that the UREs were cooperative throughout the compliance enforcement process;
3. The UREs had a compliance program at the time of the violation which Reliability*First* considered a mitigating factor, as discussed in the Disposition Documents;
4. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. URE 1 and URE 2 submitted the Mitigation Plan for Violation IDs: RFC201000226, RFC201000229, RFC201000227, RFC201000230, RFC201000228, and RFC201000231 prior to the "Compliant." In consideration of URE 1 and URE 2's prompt preparation, drafting, and submittal of the Mitigation Plan, Reliability*First* assessed a zero dollar penalty for these violations as discussed in the Disposition Documents;
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 one hundred eighty thousand dollars ($180,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

---

[12] *See* 18 C.F.R. § 39.7(d)(4).

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

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 the UREs executed April 12, 2011, included as Attachment a;
    i. URE 1 and URE 2's Violation Self-Reporting Form for RFC201000226, RFC201000227, RFC201000229, and RFC201000230, included as Attachment A to the Settlement Agreement;
    ii. URE 1 and URE 2's Mitigation Plans MIT-10-2429 and MIT-10-2438[14] for RFC201000226, RFC201000227, RFC201000228, RFC201000229, RFC201000230, and RFC201000231, included as Attachment B to the Settlement Agreement;
    iii. URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000226, RFC201000227, RFC201000228, RFC201000229, RFC201000230, and RFC201000231, included as Attachment C to the Settlement Agreement;

[14] URE 1 and URE 2 submitted one Mitigation Plan that was then assigned separate identification numbers by NERC.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

iv. Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2429 and MIT-10-2438, included as Attachment D to the Settlement Agreement;
v. URE 1 and URE 2's Violation Self-Reporting Form for RFC201000228 and RFC201000231, included as Attachment E to the Settlement Agreement;
vi. URE 1 and URE 2's Violation Self-Reporting Form for RFC201000424 and RFC201000425, included as Attachment F to the Settlement Agreement;
vii. URE 1 and URE 2's Mitigation Plans MIT-10-2782 and MIT-10-2783[15] for RFC201000424 and RFC201000425, included as Attachment G to the Settlement Agreement;
viii. URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000424 and RFC201000425, included as Attachment H to the Settlement Agreement;
ix. Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2782 and MIT-10-2783, included as Attachment I to the Settlement Agreement;
x. URE 1 and URE 2's Violation Self-Reporting Form for RFC201000594 and RFC201000600, included as Attachment J to the Settlement Agreement;
xi. URE 1 and URE 2's Mitigation Plans MIT-10-2906 for RFC201000594 and RFC201000600, included as Attachment K to the Settlement Agreement;
xii. URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000594 and RFC201000600, included as Attachment L to the Settlement Agreement;
xiii. Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2906, included as Attachment M to the Settlement Agreement;
xiv. URE 1 and URE 2's Violation Self-Reporting Form for RFC201000595 and RFC201000601, included as Attachment N to the Settlement Agreement;
xv. URE 1 and URE 2's Mitigation Plans MIT-10-2907 for RFC201000595 and RFC201000601, included as Attachment O to the Settlement Agreement;
xvi. URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000595 and RFC201000601, included as Attachment P to the Settlement Agreement;
xvii. Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2907, included as Attachment Q to the Settlement Agreement;
xviii. URE 1 and URE 2's Violation Self-Reporting Form for RFC201000596 and RFC201000602, included as Attachment R to the Settlement Agreement;
xix. URE 1 and URE 2's Mitigation Plans MIT-10-3024 for RFC201000596 and RFC201000602, included as Attachment S to the Settlement Agreement;

[15] URE 1 and URE 2 submitted one Mitigation Plan that was then assigned separate identification numbers by NERC.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

xx. URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000596 and RFC201000602, included as Attachment T to the Settlement Agreement;

xxi. ReliabilityFirst's Verification of Mitigation Plan Completion for MIT-10-3024, included as Attachment U to the Settlement Agreement;

xxii. URE 1 and URE 2's Violation Self-Reporting Form for RFC201000597 and RFC201000603, included as Attachment V to the Settlement Agreement;

xxiii. URE 1 and URE 2's Mitigation Plans MIT-10-2915 for RFC201000597 and RFC201000603, included as Attachment W to the Settlement Agreement;

xxiv. URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000597 and RFC201000603, included as Attachment X to the Settlement Agreement;

xxv. ReliabilityFirst's Verification of Mitigation Plan Completion for MIT-10-2915, included as Attachment Y to the Settlement Agreement;

xxvi. URE 1 and URE 2's Violation Self-Reporting Form for RFC201000598 and RFC201000604, included as Attachment Z to the Settlement Agreement;

xxvii. URE 1 and URE 2's Mitigation Plans MIT-10-2916 for RFC201000598 and RFC201000604, included as Attachment AA to the Settlement Agreement;

xxviii. URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000598 and RFC201000604, included as Attachment BB to the Settlement Agreement;

xxix. ReliabilityFirst's Verification of Mitigation Plan Completion for MIT-10-2916, included as Attachment CC to the Settlement Agreement;

xxx. URE 1 and URE 2's Violation Self-Reporting Form for RFC201000599 and RFC201000605, included as Attachment DD to the Settlement Agreement;

xxxi. URE 1 and URE 2's Mitigation Plans MIT-10-2917 for RFC201000599 and RFC201000605, included as Attachment EE to the Settlement Agreement;

xxxii. URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000599 and RFC201000605, included as Attachment FF to the Settlement Agreement;

xxxiii. ReliabilityFirst's Verification of Mitigation Plan Completion for MIT-10-2917, included as Attachment GG to the Settlement Agreement;

xxxiv. URE 1 and URE 2's Violation Self-Reporting Form for RFC201100726, RFC201100727, RFC201100729, and RFC201100730, included as Attachment HH to the Settlement Agreement;

xxxv. URE 1 and URE 2's Mitigation Plans MIT-10-3421 for RFC201100726, RFC201100727, RFC201100729, and RFC201100730, included as Attachment II to the Settlement Agreement;

xxxvi. URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201100726, RFC201100727, RFC201100729, and RFC201100730, included as Attachment JJ to the Settlement Agreement;

xxxvii. URE 1 and URE 2's Violation Self-Reporting Form for RFC201100728 and RFC201100731, included as Attachment KK to the Settlement Agreement;

xxxviii. URE 1 and URE 2's Mitigation Plans MIT-10-3422 for RFC201100728 and RFC201100731, included as Attachment LL to the Settlement Agreement;

xxxix. URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201100728 and RFC201100731, included as Attachment MM to the Settlement Agreement;

xl. URE 1's Violation Self-Reporting Form for RFC201000661, included as Attachment NN to the Settlement Agreement;[16]

xli. URE 1 and URE 2's Mitigation Plans MIT-10-3316 for RFC201000661, included as Attachment OO to the Settlement Agreement;

xlii. URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000661, included as Attachment PP to the Settlement Agreement;

xliii. Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-3316, included as Attachment QQ to the Settlement Agreement;

xliv. URE 3's Violation Self-Reporting Form for RFC201100732, included as Attachment RR to the Settlement Agreement;

xlv. URE 3's Mitigation Plans MIT-10-3423 for RFC201100732, included as Attachment SS to the Settlement Agreement;

xlvi. URE 3's Certification of Mitigation Plan Completion for RFC201100732, included as Attachment TT to the Settlement Agreement;

b) Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-3421, included as Attachment b to the Settlement Agreement;

c) Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-3422, included as Attachment c to the Settlement Agreement;

d) Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-3423, included as Attachment d to the Settlement Agreement;

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

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

ii. Disposition Document for CIP-005, included as Attachment e-2;

iii. Disposition Document for CIP-006, included as Attachment e-3; and

iv. Disposition Document for CIP-007, included as Attachment e-4.

A Form of Notice Suitable for Publication[17]

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

[16] URE 1 submitted a Self-Report for a violation of CIP-004-2 R4. Upon further review, Reliability*First* determined that the facts instead indicated a violation of CIP-007-2 R5.2.3.

[17] *See* 18 C.F.R. § 39.7(d)(6).

Notices and Communications

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

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

*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Rebecca J. Michael*
Associate General Counsel for Corporate and Regulatory Matters
Sonia C. Mendonca*
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.medonca@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

Amanda E. Fried*
Associate Attorney
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
amanda.fried@rfirst.org

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

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

Respectfully submitted,

/s/ *Rebecca J. Michael*

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

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Sonia C. Mendonca
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.medonca@nerc.net

cc: Unidentified Registered Entity 1
Unidentified Registered Entity 3
Unidentified Registered Entity 2
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 July 11, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity 1 (URE 1)	**NCRXXXXX**	**NOC-857**
Unidentified Registered Entity 3 (URE 3)	**NCRXXXXX**	
Unidentified Registered Entity 2 (URE 2)	**NCRXXXXX**	
(Collectively, the UREs)		

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 **$180,000** FOR **28** 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

[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.

ADDITIONAL COMMENTS
Some of the violations addressed in the Settlement Agreement constituted repetitive conduct and were aggravating factors in Reliability*First*'s penalty determination. After the first occurrences of CIP-004, CIP-005, CIP-006, and CIP-007, the additional violations of those Standards were considered as constituting repetitive conduct attributable to the same compliance program and were aggravating factors in penalty determination.[2]

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

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

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ NO ☐ UNDETERMINED ☐
EXPLAIN
Reliability*First* considered certain aspects of the UREs' compliance program as mitigating factors.

[2] CIP-004-1 R4.2 (RFC201000595 and RFC201000601), CIP-005-1 R1 (RFC201000596 and RFC201000602), CIP-006-2 R1 (RFC201000597 and RFC201000603), CIP-007-2a R1(RFC201000598 and RFC201000604), CIP-007-2 R3.1 (RFC201000599 and RFC201000605), CIP-007-2 R5.2.3 (RFC201000661), CIP-004-2 R2 and R3(RFC201100726, RFC201100727, RFC201100729, and RFC201100730), CIP-004-2 R4 (RFC201100728 and RFC201100731), and CIP-004-3 R3 (RFC201100732).

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
URE 1 and URE 2 submitted the Mitigation Plan for Violation IDs: RFC201000226, RFC201000229, RFC201000227, RFC201000230, RFC201000228, and RFC201000231 prior to the Compliant date. In consideration of URE 1 and URE 2's prompt preparation, drafting, and submittal of the Mitigation Plan, Reliability*First* assessed a zero dollar penalty for these violations.

(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: **2/8/11**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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment e-1

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000594: URE 1	**RFC201000594**
RFC201000595: URE 1	**RFC201000595**
RFC201000600: URE 2	**RFC201000600**
RFC201000601: URE 2	**RFC201000601**
RFC201100726: URE 1	**300781**
RFC201100727: URE 1	**300782**
RFC201100728: URE 1	**300783**
RFC201100729: URE 2	**300784**
RFC201100730: URE 2	**300785**
RFC201100731: URE 2	**300786**
RFC201100732: URE 3	**300787**

I. VIOLATION INFORMATION

Violation ID	RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
RFC201000594	**CIP-004-2**	**2**	**2.1**	**Medium** [1]	**Lower**[2]
RFC201000595	**CIP-004-1**	**4**	**4.2**	**Medium** [3]	**N/A**[4]
RFC201000600	**CIP-004-2**	**2**	**2.1**	**Medium**	**Lower**
RFC201000601	**CIP-004-1**	**4**	**4.2**	**Medium**	**N/A**
RFC201100726	**CIP-004-2**	**2**		**Medium**	**Lower**
RFC201100727	**CIP-004-2**	**3**		**Medium** [5]	**High**
RFC201100728	**CIP-004-2**	**4**		**Medium**	**Moderate**
RFC201100729	**CIP-004-2**	**2**		**Medium**	**Lower**
RFC201100730	**CIP-004-2**	**3**		**Medium**	**High**
RFC201100731	**CIP-004-2**	**4**		**Medium**	**Moderate**
RFC201100732	**CIP-004-3**	**3**		**Medium**	**High**[6]

[1] CIP-004 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a Lower Violation Risk Factor (VRF); R2.1, R2.2 and R2.2.4 each have a Medium VRF.
[2] On December 18, 2009, NERC submitted revised VRFs and Violation Severity Levels (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 for RFC201000594, RFC201100726, RFC201100727, RFC201100728, RFC201100729, RFC201100730, and RFC201100731.
[3] CIP-004-1 R4 and R4.1 each have a Lower VRF; R4.2 has a Medium VRF.
[4] At the time of the violations, no VSLs were in effect for CIP-004-1 (RFC201000595 and RFC201000601). 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.
[5] CIP-004 R3 has a Medium VRF; R3.1, R3.2 and R3.3 each have a Lower VRF.

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

The purpose statement of CIP-004 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. [7]

CIP-004-1 R4 provides:

> **R4. Access — The Responsible Entity[8] shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.**
>
> > **R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.**
> >
> > **R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.**

(Footnote added.)

CIP-004-2 provides in pertinent part:

> **R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted**

---

[6] 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 for RFC201100732.
[7] The Purpose Statement of Version Two of the Reliability Standard refers to CIP-004-2 and Version Three refers to CIP-004-3.
[8] 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.

physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access 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:

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.

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

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

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

CIP-004-3 R3 provides:

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:

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-004-3.

VIOLATION DESCRIPTIONS

CIP-004-1 R2.1 (RFC201000594 and RFC201000600)
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-004-2 R2.1. URE 1 and URE 2 discovered that two of their security command center operators mistakenly allowed a new security officer, who had a valid Personnel Risk Assessment (PRA) but had not yet completed cyber security training, to enter a PSP housing Critical Cyber Assets (CCAs) on 18 occasions. URE 1's and URE 2's access control programs require that individuals have both a valid PRA and cyber security training prior to being granted authorized cyber or unescorted physical access to CCAs. Accordingly, the security officer's unescorted physical access to CCAs was unauthorized because the security officer had not yet completed the requisite cyber security training.

CIP-004-1 R4.2 (RFC201000595 and RFC201000601)
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-004-2 R4.2. URE 1 and URE 2 discovered that they failed to revoke the physical access rights of an individual who no longer required such access once they were required to comply with CIP-004-1 R4.2. In July 2008, UREs granted an information services department individual physical access rights to various restricted locations containing CCAs. The individual transferred positions on October 6, 2008 and no longer required such access. Due to oversight, URE 1 and URE 2 failed to revoke the individual's access rights within seven calendar days of

the transfer. URE 1 and URE 2 revoked the individual's access rights on June 28, 2010.

CIP-004-2 R2 (RFC201100726 and RFC201100729)
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-004-2 R2. Due to URE 1's and URE 2's weekday daily reconciliation process for reviewing access, URE 1 and URE 2 discovered that they failed to train an individual with unescorted access to CCAs prior to that individual gaining such access, in violation of CIP-004-2 R2.1. The individual required unescorted physical access to a location for which cyber security training was not required. This location was located within a PSP containing CCAs and in order to access this location, the individual also required access to the PSP containing CCAs. Personnel submitted requests for access to each of these locations for the individual. URE 1 and URE 2 processed the request for access to the necessary location first because the individual had not yet completed training for the PSP access request. URE 1 and URE 2 mistakenly granted unescorted physical access to the PSP location and not the necessary location, thus providing the individual unauthorized physical access to the PSP containing CCAs. URE 1 and URE 2 granted physical access despite this individual not yet completing cyber security training nor having a completed PRA.

CIP-004-2 R3 (RFC201100727 and RFC201100730)
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-004-2 R3. Regarding the same individual as discussed in the description of the alleged violations of CIP-004-2 R2 (RFC201100726 and RFC201100729), URE 1 and URE 2 discovered that they failed to conduct a PRA for that individual, who had access to CCAs, prior to granting that individual such access. The individual required unescorted physical access to a location for which a PRA was not required; however, this necessary location was located within a PSP containing CCAs. The individual submitted the requests for access to each of these locations. URE 1 and URE 2 mistakenly granted unescorted physical access to the PSP location and not the necessary location, thus providing the individual with unauthorized physical access to the PSP containing the CCAs.

CIP-004-2 R4 (RFC201100728 and RFC201100731)
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-004-2 R4. URE 1 and URE 2 discovered that they failed to revoke the physical access rights of an individual who no longer required such access. Due to a change in job responsibilities, an individual with physical access rights to a location containing CCAs no longer required such access, but due to an error in writing and processing the request, URE 1 and URE 2 failed to revoke the individual's access rights within seven calendar days of the transfer. URE 1 and URE 2 revoked the individual's access rights on November 22, 2010.

CIP-004-3 R3 (RFC201100732)
The violation of CIP-004-3 R3 is by URE 3 only. URE 3 submitted a Self-Report to Reliability*First* identifying a violation of CIP-004-3 R3. URE 3 discovered that it mistakenly granted an individual unescorted physical access to a PSP prior to that individual having a completed PRA, in violation of CIP-004-3 R3. URE 3 granted the individual access to only the PSP at the URE 3 facility, and the individual entered unescorted prior to completing a PRA three times on a single date, November 19, 2010.

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-004-1 R2.1 (RFC201000594 and RFC201000600)
At the time of the incidents, the security officer had a valid PRA. Additionally, the security officer subsequently completed the requisite training, and URE 1 and URE 2 then granted the officer unescorted physical access to CCAs. The officer has since resigned.

CIP-004-1 R4.2 (RFC201000595 and RFC201000601)
The individual did not access the location containing CCAs after transferring positions, and at all relevant times, the individual had CIP clearance. In addition, the individual remains employed by UREs.

CIP-004-2 R2 (RFC201100726 and RFC201100729) and CIP-004-2 R3 (RFC201100727 and RFC201100730)
URE 1 and URE 2 initially approved the individual's access for only 13 hours, during which the individual did not in fact access the PSP containing CCAs. Moreover, the process in place to verify correct access authorization promptly permitted URE 1 and URE 2 to identify and eliminate the incorrectly authorized access before any access actually occurred. Specifically, the corporate security review process facilitated correction of the issue in a time period shorter than the 24 hours allotted for removing access in other contexts. In addition, URE 1 and URE 2 had previously granted this individual access to certain noncritical areas since September 2007, in the individual's role of supporting the facilities management organization. During the time period that the individual had such access, there was no security event associated with the individual.

CIP-004-2 R4 (RFC201100728 and RFC201100731)
The individual at issue has worked for URE for nearly 33 years and had a valid PRA and cyber security training. The individual did not access the PSP containing CCAs after no longer requiring such access. Furthermore, the individual retains access to other NERC PSPs for current job responsibilities.

CIP-004-3 R3 (RFC201100732)
The individual had current cyber security training, and URE 3 approved the PRA four days after mistakenly granting access. URE 3 granted the individual access to only the PSP at the URE 3 facility, and the individual entered unescorted prior to completing a PRA three times on a single date, November 19, 2010. The individual has a valid PRA in place, is still engaged as a contract worker for URE 3, and retains access to the PSP.

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-004-1 R2.1 (RFC201000594 and RFC201000600)
6/16/10 through 6/22/10 (when URE 1 and URE 2 identified the issue and refused CCA access to the officer until the officer completed all training)

CIP-004-1 R4.2 (RFC201000595 and RFC201000601)
1/1/10 through 6/28/10 (when URE 1 and URE 2 revoked the individual's access)

CIP-004-2 R2 (RFC201100726 and RFC201100729)
CIP-004-2 R3 (RFC201100727 and RFC201100730)
7/20/10 (when URE 1 and URE 2 granted the individual access rights) through 7/21/10 (when URE 1 and URE 2 revoked access rights)

CIP-004-2 R4 (RFC201100728 and RFC201100731)
6/16/10 (when the individual no longer required access) through 11/22/10 (when URE 1 and URE 2 revoked access rights)

CIP-004-3 R3 (RFC201100732)
11/18/10 (when URE 3 granted access to the individual) through 11/22/10 (when the individual had a completed PRA)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

CIP-004-1 R2.1 (RFC201000594 and RFC201000600)
CIP-004-1 R4.2 (RFC201000595 and RFC201000601): Self-Report

CIP-004-2 R2 (RFC201100726 and RFC201100729)
CIP-004-2 R3 (RFC201100727 and RFC201100730)
CIP-004-2 R4 (RFC201100728 and RFC201100731)
CIP-004-3 R3 (RFC201100732): **Self-Report**

ARE THE VIOLATIONS STILL OCCURRING YES ☐ NO ☒
IF YES, EXPLAIN

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

III. MITIGATION INFORMATION

CIP-004-1 R2.1 (RFC201000594 and RFC201000600)
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2906**
DATE SUBMITTED TO REGIONAL ENTITY	**8/31/10**
DATE ACCEPTED BY REGIONAL ENTITY	**9/24/10**
DATE APPROVED BY NERC	**10/12/10**
DATE PROVIDED TO FERC	**10/12/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**7/30/10**
DATE OF CERTIFICATION LETTER	**1/19/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**7/30/10**
DATE OF VERIFICATION LETTER	**2/8/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**7/30/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
At URE 1's and URE 2's direction, the third-party contractor revised its on-boarding procedure to ensure that all new contract security officers attain a valid PRA and complete required training before authorizing unescorted physical access. URE 1 and URE 2 reviewed the incident with security command center operators and reinforced responsibilities for following

cyber security procedures. URE 1 and URE 2 granted unescorted physical access to the officer only after the officer completed cyber security training.

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

- **Complete cyber security training for the new security officer - Evidence Provided: Photocopy of training record contained in UREs' automated training program showing training for new officer was completed.**
- **Grant new security officer unescorted physical access to PSPs - Evidence Provided: Photocopy of log granting physical access to new officer on June 25, 2010, no date.**
- **Photocopy of Corrective Action Form from vendor company for security officers used at URE indicating results of counseling session with subject employees, dated June 30, 2010, July 2, 2010, and July 24, 2010**
- **Conduct stand down meeting with Operators - Evidence Provided: Memo which reviews process and procedure for granting unescorted physical access to UREs' PSP. Employees were required to read and sign memo as attestation of compliance.**
- **Copy of new-hire checklist for UREs Locations, dated July 30, 2010, indicating revisions**

CIP-004-1 R4.2 (RFC201000595 and RFC201000601)
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2907**
DATE SUBMITTED TO REGIONAL ENTITY	**8/31/10**
DATE ACCEPTED BY REGIONAL ENTITY	**9/24/10**
DATE APPROVED BY NERC	**10/12/10**
DATE PROVIDED TO FERC	**10/12/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**7/9/10**
DATE OF CERTIFICATION LETTER	**1/19/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**7/9/10**

DATE OF VERIFICATION LETTER	**2/7/11**[9]
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**7/9/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE 1 and URE 2 revoked the individual's access and counseled management personnel to ensure a clear understanding of CIP responsibilities. UREs revised the process for reviewing personnel transfers across departments which provides an additional safeguard to ensure that it properly revokes 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)

- **Implement process to review all department transfers for access revocation Evidence Provided: Memo attesting to the completion of Milestone Activity D.3.a with the implementation, personnel change status process which combines NERC CIP, FERC, and related accesses in order to better control timely authorization and removal of access privileges, dated January 3, 2011.**
- **Remove the individual's unescorted physical access to PSP Evidence Provided: Photocopy of journal indicating removal of authorization of subject employee on 06/28/2010.**
- **Counseled the subject employees and prior supervisor to ensure a clear understanding of the need to identify and remove all NERC CIP accesses when an individual departs the work group. Evidence Provided: Memo attesting to the discussions and conversations in person and by telephone as well as emails with the subject employees prior supervisor emphasizing the importance**

CIP-004-2 R2 (RFC201100726 and RFC201100729)
CIP-004-2 R3 (RFC201100727 and RFC201100730)
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-3421**
DATE SUBMITTED TO REGIONAL ENTITY	**1/21/11 (signed 1/6/11)**
DATE ACCEPTED BY REGIONAL ENTITY	**2/16/11**
DATE APPROVED BY NERC	**3/16/11**
DATE PROVIDED TO FERC	**3/16/11**

[9] The Verification of Mitigation Plan Completion has a typographical error that states the Mitigation Plan for the CIP-004-1 R4.2 violations (RFC201000595 and RFC201000601) was completed as of July 30, 2010.

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**3/31/11**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**1/25/11**
DATE OF CERTIFICATION LETTER	**3/28/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**1/25/11**
DATE OF VERIFICATION LETTER	**4/28/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**1/25/11**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE 1 and URE 2 revoked the individual's access within 13 hours of granting it. In addition, URE 1 and URE 2 counseled and trained the relevant employees regarding the access granting procedures. URE 1 and URE 2 reconfigured the location at issue to separate the PSP containing CCAs from the location that does not require a PRA and training to gain 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)

- **Printout dated July 21, 2010 of URE 1 and URE 2 evidence document**
- **Corrective Action Form dated July 21, 2010 of URE 1 and URE 2 evidence document**
- **Attestation of review of erroneous granting unescorted access to a critical area by supervisor dated January 1, 2011 of URE 1 and URE 2 evidence document**
- **Attestation Memo of URE 1 and URE 2 evidence document**

CIP-004-2 R4 (RFC201100728 and RFC201100731)

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-3422**
DATE SUBMITTED TO REGIONAL ENTITY	**1/21/11 (signed 1/6/11)**
DATE ACCEPTED BY REGIONAL ENTITY	**2/16/11**
DATE APPROVED BY NERC	**3/16/11**
DATE PROVIDED TO FERC	**3/16/11**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**11/23/10**
DATE OF CERTIFICATION LETTER	**3/28/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**11/23/10**
DATE OF VERIFICATION LETTER	**5/2/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**11/23/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE 1 and URE 2 revoked the individual's access upon discovery. In addition, URE 1 and URE 2 counseled and trained the relevant employees regarding the access revocation procedures.

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)

- **Printout dated November 22, 2010 of URE 1 and URE 2 Evidence document. This document provides evidence that the employee who was supposed to have physical access to PSP revoked on June 16, 2010 had access revoked on November 22, 2010.**
- **Corrective Action Form dated November 22, 2010 provides evidence the operator that failed to revoke access for the transferred employee was counseled to ensure clear understanding of the access approval process.**
- **Attestation Memo provided evidence through an attestation that on November 23, 2010 a tailboard training session was held with all operators to review the access approval process.**

CIP-004-3 R3 (RFC201100732)

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-3423**
DATE SUBMITTED TO REGIONAL ENTITY	**1/21/11 (signed 1/6/11)**
DATE ACCEPTED BY REGIONAL ENTITY	**2/16/11**
DATE APPROVED BY NERC	**3/16/11**
DATE PROVIDED TO FERC	**3/16/11**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **12/22/10**

DATE OF CERTIFICATION LETTER **3/29/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **12/22/10**

DATE OF VERIFICATION LETTER **5/2/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **12/22/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE 3 approved the individual's PRA and trained the individuals responsible for granting CIP clearance, including the specific individual who mistakenly granted access leading to this violation. URE 3 replaced security command center operators with specifically trained corporate security administrative staff members as the individuals responsible for granting unescorted physical access to PSPs.

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)
These documents provide evidence that the contractor that was granted access to PSP had a PRA completed:

- **Email dated November 23, 2010 of URE 3 evidence document**
- **Security Officer's action to remove operators from granting unescorted access dated December 1, 2010**
- **Incident History Form dated December 1, 2010**
- **Corporate Security's instruction procedure for administrative staff**
- **Corporate Security's instruction procedure for operators**

These documents provide evidence that the following steps were performed to mitigate any future violation of CIP-004-3 R3:

- **Email dated November 23, 2010 provides evidence of an email training notification to the administrative staff and operator going over the steps required to check for a completed PRA before granting access.**

- **Security Officer's action to remove operators from granting unescorted access dated December 1, 2010 of URE 3 evidence document provided evidence of a change request issued to change the unescorted physical access request process to remove the operators from the group that can grant unescorted access to any PSP and to Restrict this function to Corporate Security administrative staff members, who are part of a smaller group specifically knowledgeable of the NERC CIP clearance process.**
- **Incident History Form dated December 1, 2010 of URE 3 evidence document provides evidence the Security administrative individual that granted access to the contract worker was counseled to ensure clear understanding of the instruction for checking on PRA completion during the access approval process.**
- **Corporate Security's instruction procedure for administrative staff provide evidence of updates to the administrative staff instructions and the operator instructions for processing security requests for unescorted physical access.**

EXHIBITS:

SOURCE DOCUMENTS

URE 1 and URE 2's Violation Self-Reporting Form for RFC201000594 and RFC201000600

URE 1 and URE 2's Violation Self-Reporting Form for RFC201000595 and RFC201000601

URE 1 and URE 2's Violation Self-Reporting Form for RFC201100726, RFC201100727, RFC201100729, and RFC201100730

URE 1 and URE 2's Violation Self-Reporting Form for RFC201100728 and RFC201100731

URE 3's Violation Self-Reporting Form for RFC201100732

MITIGATION PLANS

URE 1 and URE 2's Mitigation Plans MIT-10-2906 for RFC201000594 and RFC201000600

URE 1 and URE 2's Mitigation Plans MIT-10-2907 for RFC201000595 and RFC201000601

URE 1 and URE 2's Mitigation Plans MIT-10-3421 for RFC201100726, RFC201100727, RFC201100729, and RFC201100730

URE 1 and URE 2's Mitigation Plans MIT-10-3422 for RFC201100728 and RFC201100731

URE 3's Mitigation Plans MIT-10-3423 for RFC201100732

CERTIFICATIONS BY REGISTERED ENTITIES

URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000594 and RFC201000600

URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000595 and RFC201000601
URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201100726, RFC201100727, RFC201100729, and RFC201100730

URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201100728 and RFC201100731
URE 3's Certification of Mitigation Plan Completion for RFC201100732

VERIFICATIONS BY REGIONAL ENTITY

Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2906 for RFC201000594 and RFC201000600

Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2907

Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-3421 for RFC201100726, RFC201100727, RFC201100729, and RFC201100730

Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-3422 for RFC201100728 and RFC201100731

Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-3423 for RFC201100732

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-005

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment e-2

DISPOSITION OF VIOLATION

Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000226: URE 1	**RFC201000226**
RFC201000227: URE 1	**RFC201000227**
RFC201000229: URE 2	**RFC201000229**
RFC201000230: URE 2	**RFC201000230**
RFC201000596: URE 1	**RFC201000596**
RFC201000602: URE 2	**RFC201000602**

I. VIOLATION INFORMATION

VIOLATION ID	RELIABILITY STANDARD[1]	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
RFC201000226	**CIP-005-1**	**2**		**Medium**[2]	**N/A**[3]
RFC201000227	**CIP-005-1**	**3**		**Medium**	**N/A**
RFC201000229	**CIP-005-1**	**2**		**Medium**	**N/A**
RFC201000230	**CIP-005-1**	**3**		**Medium**	**N/A**
RFC201000596	**CIP-005-1**	**1**		**Medium**[4]	**N/A**
RFC201000602	**CIP-005-1**	**1**		**Medium**	**N/A**

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 provides:

> **The Responsible Entity[5] shall comply with the following requirements of Standard CIP-005:**

[1] Some of the supporting documents refer to these violations as violations of the CIP-005-2 or CIP-005-2a versions of the Reliability Standard.
[2] 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.
[3] 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.
[4] CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a Medium VRF; R1.6 has a Lower VRF.

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

---

[5] 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

R2. Electronic Access Controls — The Responsible Entity 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).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

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.

> **R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.**
>
> > **R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.**
> >
> > **R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.**

(Footnote added.)

VIOLATION DESCRIPTION

Background information common to Violation IDs RFC201000226, RFC201000229, RFC201000227, and RFC201000230:

The URE Entities' information services department protects both URE 1's transmission management system and URE 2's generation management system, with a single, continuous Electronic Security Perimeter (ESP) spanning multiple Physical Security Perimeters (PSPs). The URE Entities hired consultants to ensure compliance with CIP Standards by its Compliant date. The consulting firm conducted a mock audit of the URE Entities' compliance which revealed that the URE Entities' single, continuous ESP possibly violated numerous CIP Standards.

CIP-005-1 R2 (RFC201000226 and RFC201000229)
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-005-1 R2. There are nine access points to the ESP related to the networks that provide UREs' telecommunications services for which URE 1 and URE 2 did not have proper access control. Specifically, at the nine access points, URE 1 and URE 2 failed to implement an access control model that denies access by default, as required by CIP-005-1 R2.1. The continuous ESP also caused URE 1 and URE 2 to fail to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP at the access points and document that configuration, as required by CIP-005-1 R2.2.

CIP-005-1 R3 (RFC201000227 and RFC201000230)
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-005-1 R3. URE 1 and URE 2 discovered that by not designating multiple ESPs, they failed to implement proper logging at all access points to the ESP. Specifically, URE 1 and URE 2 failed to implement logging at the nine access points for which they did not have proper access control because there were no firewalls at these access points to monitor access.

CIP-005-1 R1 (RFC201000596 and RFC201000602)
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-005-1 R1. URE 1 and URE 2 discovered that they failed to identify two non-critical Cyber Assets within the ESP and failed to identify one Cyber Asset as an access point to the ESP. During a comprehensive review of the ESP and PSPs, the information services department discovered that it had also not identified two URE 1 and URE 2 servers connected to the transmission management system and generation management system network as application servers. Because the two servers were not application servers, in accordance with UREs' methodology, the two servers were non-critical Cyber Assets. URE 1 and URE 2 therefore failed to identify these two servers as non-critical Cyber Assets within the ESP, in violation of CIP-005-1 R1.4. In addition, during the comprehensive review of the ESP and PSPs, URE 1 and URE 2 discovered a low tension network monitoring device within the ESP. URE 1 and URE 2 installed this device as part of a project to monitor the low tension distribution network, but that project was deferred, rendering the Cyber Asset non-critical pursuant to UREs' methodology. URE 1 and URE 2 failed to identify this device both as an access point to the ESP, in violation of CIP-005-1 R1, and as a non-critical Cyber Asset, in violation of CIP-005-1 R1.4.

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-005-1 R2 (RFC201000226 and RFC201000229) and CIP-005-1 R3 (RFC201000227 and RFC201000230)
The communications assets associated with the access points are physically protected even though not all reside within a PSP. In addition, the transmission management system and the generation management system are both connected to network systems that utilize network monitoring protections as well as Level-1 non-routable protocols. Consequently, the network systems do not communicate outside of UREs. Additionally, a support vendor monitors the network systems 24 hours a day, seven days a week. The network systems also utilize programs, including redundant protection, which alert URE 1 and URE 2 to anomalies or security issues. Furthermore, connections to the network systems are password-protected. The above factors contribute to the security of the UREs' corporate system and the unlikelihood that an unauthorized user could gain access to the network systems,

including, but not limited to, the transmission management system and the generation management system.

CIP-005-1 R1 (RFC201000596 and RFC201000602)
The servers at issue resided within the ESP and a PSP and had the protections required by the remainder of CIP-005. In addition, the servers were equipped with up to date anti-virus software, security patches, and CIP-compliant managed accounts. The device at issue did not use the internet for communication, and communicated outside the ESP using only a routable protocol over dedicated cable. Due to these physical components, it would be difficult for an unauthorized user to gain access to UREs' system.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S)
CIP-005-1 R2 (RFC201000226 and RFC201000229)
CIP-005-1 R3 (RFC201000227 and RFC201000230)
1/1/10 through 12/23/10 (Mitigation Plan completion)

CIP-005-1 R1 (RFC201000596 and RFC201000602)
1/1/10 through 8/25/10 (when URE 1 and URE 2 disconnected the last device from the ESP)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

CIP-005-1 R2 (RFC201000226 and RFC201000229)
CIP-005-1 R3 (RFC201000227 and RFC201000230) Self-Report

CIP-005-1 R1 (RFC201000596 and RFC201000602) Self-Report

ARE THE VIOLATIONS STILL OCCURRING YES ☐ NO ☒
IF YES, EXPLAIN

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

III. MITIGATION INFORMATION

CIP-005-1 R2 (RFC201000226 and RFC201000229)
CIP-005-1 R3 (RFC201000227 and RFC201000230)
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2429 and MIT-10-2438**[6]
DATE SUBMITTED TO REGIONAL ENTITY	**12/31/09**
DATE ACCEPTED BY REGIONAL ENTITY	**3/31/10**
DATE APPROVED BY NERC	**4/16/10**
DATE PROVIDED TO FERC	**4/16/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**12/23/10**
DATE OF CERTIFICATION LETTER	**1/6/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**12/23/10**
DATE OF VERIFICATION LETTER	**2/15/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**12/23/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE 1 upgraded its transmission management system with a system that included the installation of firewalls and the creation of separate ESPs at various access points to the new transmission management system. The replacement transmission management system also resolved URE 2's generation management system issue due to the use of common network components. URE 2 installed additional firewalls at access points to the generation management system and URE 2 upgraded switches and installed firewalls so that the links between discrete ESPs were protected from intrusion.

[6] Although NERC assigned separate ID numbers for URE 1's and URE 2's Mitigation Plan, URE 1 and URE 2 only submitted one Mitigation Plan. This Mitigation Plan also includes the CIP-006-R1.1 violations (RFC201000228 and RFC201000231) which are addressed in a separate Disposition Document.

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)

- **UREs provided evidence that shows the re-architecture needs and implementation schedule for the transmission management system replacement.**
- **Evidence that determines its re-architecture needs and implementation schedule for the transmission management system replacement and the generation management system resolution for workstation and communication services component, including required additional firewalls.**
- **Evidence that shows the revised implementation schedule for the transmission management system replacement and generation management system resolution of the additional firewalls.**
- **Evidence that shows the factory acceptance testing for the component of the transmission management system replacement and the mitigation plan for the switch architecture with a network design and communication equipment.**
- **Evidence that shows the UREs completing lab/development configuration and testing of the new transmission management system site to site firewall design.**
- **Evidence that shows the completion of lab/development configuration testing of the generation management system firewall design. .**
- **Evidence that shows the completion of the installation of the redesigned transmission management system network with the required firewalls and the complete site acceptance testing for the component of the transmission management system replacement.**
- **Evidence that shows the installation testing and cut over to the new transmission management system.**
- **Evidence that shows the installation of the required generation management system firewalls and complete installation testing.**

CIP-005-1 R1 (RFC201000596 and RFC201000602)

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-3024**
DATE SUBMITTED TO REGIONAL ENTITY	**9/29/10 (signed 9/27/10)**
DATE ACCEPTED BY REGIONAL ENTITY	**10/22/10**
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 **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **9/22/10**

DATE OF CERTIFICATION LETTER **1/19/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **9/22/10**

DATE OF VERIFICATION LETTER **1/28/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **9/22/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE 1 and URE 2 disconnected the two servers and the device from the network. URE 1 and URE 2 also completed a comprehensive review of the ESP and PSPs and found no irregularities.

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 the two unused servers were removed from the network on July 16, 2010.**
- **A document that provides evidence that the unused device was removed from the network on August 25, 2010.**
- **A document that provides evidence that URE 1 and URE 2 completed their comprehensive review of all cyber assets connected within their ESPs and found only the three devices covered in the resulting Self Report.**

EXHIBITS:

SOURCE DOCUMENT
URE 1 and URE 2's Violation Self-Reporting Form for RFC201000226, RFC201000227, RFC201000229, and RFC201000230

URE 1 and URE 2's Violation Self-Reporting Form for RFC201000596 and RFC201000602

MITIGATION PLAN
URE 1 and URE 2's Mitigation Plans MIT-10-2429 and MIT-10-2438 for RFC201000226, RFC201000227, RFC201000229, and RFC201000230

URE 1 and URE 2's Mitigation Plans MIT-10-3024 for RFC201000596 and RFC201000602

CERTIFICATION BY REGISTERED ENTITY
URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000226, RFC201000227, RFC201000229, and RFC201000230

URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000596 and RFC201000602

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2429 and MIT-10-2438 for RFC201000226, RFC201000227, RFC201000229, and RFC201000230

Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-3024 for RFC201000596 and RFC201000602

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-006

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

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000228: URE 1	**RFC201000228**
RFC201000231: URE 2	**RFC201000231**
RFC201000597: URE 1	**RFC201000597**
RFC201000603: URE 2	**RFC201000603**

I. VIOLATION INFORMATION

VIOLATION ID	RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL (S)
RFC201000228	**CIP-006-1**	**1**	**1.1**	**Medium**[1]	**N/A**[2]
RFC201000231	**CIP-006-1**	**1**	**1.1**	**Medium**	**N/A**
RFC201000597	**CIP-006-2**	**1**		**Medium**	**High**[3]
RFC201000603	**CIP-006-2**	**1**		**Medium**	**High**

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."[4]

CIP-006-1 R1 provides:

> **The Responsible Entity**[5] **shall comply with the following requirements of Standard CIP-006:**

[1] CIP-006 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a Medium Violation Risk Factor (VRF); R1.7, R1.8 and R1.9 each have a Lower VRF.
[2] At the time of the violations, 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.
[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 for RFC201000597 and RFC201000603.
[4] The Purpose statement was not altered between versions CIP-006-1 and CIP-006-2.
[5] 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.

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

(Footnote added.)

CIP-006-2 R1 provides:

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).
R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

R1.6. Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

VIOLATION DESCRIPTION

CIP-006-1 R1.1 (RFC201000228 and RFC201000231)
The UREs' information services department protects both URE 1's transmission management system transmission management system and URE 2's generation management system, with a single, continuous Electronic Security Perimeter (ESP) spanning multiple Physical Security Perimeters (PSPs). Since URE 1 and URE 2 shared a single, continuous ESP, they did not have Cyber Assets associated with communication networks and data communication links between discrete ESPs. The UREs hired consultants to ensure compliance with CIP Standards by the Compliant date. The consulting firm conducted a mock audit of the UREs' compliance which revealed that the UREs' single, continuous ESP possibly violated numerous CIP Standards.

URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-006-1 R1.1. During an internal mock CIP audit conducted by outside consultants, URE 1 and URE 2 discovered that by not designating multiple ESPs, they failed to ensure that all Cyber Assets within an ESP also reside within a PSP. In one instance at URE 1's and URE 2's facility, communication links extend between two nearby buildings that were each separate PSPs, where neither a firewall nor a complete conduit[6] was in place. Since these were Cyber Assets outside of a PSP, URE 1 and URE 2 failed to create a physical security plan to ensure that the Cyber Assets within the ESP also reside within the PSP.

CIP-006-2 R1 (RFC201000597 and RFC201000603)[7]
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-006-2 R1. URE 1 and URE 2 discovered that on two separate occasions they failed to continuously escort two contract workers requiring escorted physical access to the PSP to complete their work within the PSP. First, on June 18, 2010, a URE escort left a visitor unattended in a PSP for a portion of the two hours the visitor was on the premises. That visitor did not have unescorted access rights. Second, on July 21, 2010, a URE escort did not transfer escort responsibilities for a visitor to another URE escort before leaving for the day. The visitor did not have unescorted access rights to the PSP and was unescorted for approximately one hour.

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:

[6] A complete conduit consists of wires encased in a reinforced enclosure or armored cable.
[7] Some of the supporting documents refer to these violations as violations of the CIP-006-2c version of the Reliability Standard.

CIP-006-1 R1.1 (RFC201000228 and RFC201000231)
The communications assets associated with the access points are physically protected even though not all reside within a PSP. The location of the communications assets restricted physical access. In addition, the transmission management system and the generation management system are both connected to network systems that utilize network monitoring protections as well as Level-1 non-routable protocols. Consequently, the network systems do not communicate outside of URE. Additionally, a support vendor monitors the network systems 24 hours a day, seven days a week. The network systems also utilize programs, including redundant protection, which alert URE 1 and URE 2 to anomalies or security issues. Furthermore, connections to the network systems are password-protected. The above factors contribute to the security of the URE corporate system and the unlikelihood that an unauthorized user could gain access to the network systems, including, but not limited to, the transmission management system and the generation management system.

CIP-006-2 R1 (RFC201000597 and RFC201000603)
The first visitor had a valid Personnel Risk Assessment (PRA), though the visitor had not received annual cyber security training. The second visitor was in the process of completing a PRA and cyber security training, which was completed on July 21, 2010. Thus, the two visitors posed less of a risk to UREs' system when unescorted than visitors who had no PRA or cyber security training. In addition, no cyber security events occurred during the relevant time periods.

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 R1.1 (RFC201000228 and RFC201000231)
1/1/10 through 12/23/10 (Mitigation Plan completion)

CIP-006-2 R1 (RFC201000597 and RFC201000603)
6/18/10 (date the violation occurred regarding the first visitor) and 7/21/10 (date the violation occurred regarding the second visitor)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

CIP-006-1 R1.1 (RFC201000228 and RFC201000231) **Self-Report**

CIP-006-2 R1 (RFC201000597 and RFC201000603) **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 R1.1 (RFC201000228 and RFC201000231)
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2429 and MIT-10-2438**[8]
DATE SUBMITTED TO REGIONAL ENTITY	**12/31/09**
DATE ACCEPTED BY REGIONAL ENTITY	**3/31/10**
DATE APPROVED BY NERC	**4/16/10**
DATE PROVIDED TO FERC	**4/16/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**12/23/10**
DATE OF CERTIFICATION LETTER	**1/6/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**12/23/10**
DATE OF VERIFICATION LETTER	**2/15/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**12/23/10**

[8] Although NERC assigned separate ID numbers for URE 1's and URE 2's Mitigation Plan, URE 1 and URE 2 only submitted one Mitigation Plan. This Mitigation Plan also includes the CIP-005-R2 and R3 violations (RFC201000226, RFC201000227, RFC201000229 and RFC201000230) which are addressed in a separate Disposition Document.

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE 1 replaced its transmission management system with a system that included the installation of firewalls and the creation of separate ESPs at various access points to the new transmission management system. The replacement transmission management system also resolved URE 2's generation management issue due to the use of common network components. URE 2 installed additional firewalls at access points to the generation management system and URE 2 upgraded switches and installed firewalls so that the links between discrete ESPs were protected from intrusion.

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)

- **UREs provided evidence which documents the re-architecture needs and implementation schedule for the transmission management system replacement.**
- **Evidence that determines its re-architecture needs and implementation schedule for the transmission management system replacement and the generation management system resolution for workstation and communication services component, including required additional firewalls.**
- **Evidence of the revised implementation schedule for the transmission management system replacement and generation management system resolution of additional firewalls which incorporate the information from milestone.**
- **Evidence that the factory acceptance testing for the component of the transmission management system replacement and the mitigation plan for the switch architecture with a network design and communication equipment.**
- **Evidence of completing lab/development configuration and testing of the new transmission management system site to site firewall design.**
- **Evidence of the completion of lab/development configuration testing of the generation management system firewall design.**
- **Evidence of the completion of the installation of the redesigned transmission management system network with the required firewalls and the complete site acceptance testing for the component of the transmission management system replacement.**
- **Evidence of installation testing and cut over to the new transmission management system.**
- **Evidence of the installation of the required generation management system firewalls to complete installation testing.**

CIP-006-2 R1 (RFC201000597 and RFC201000603)
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2915**
DATE SUBMITTED TO REGIONAL ENTITY	**8/31/10**
DATE ACCEPTED BY REGIONAL ENTITY	**10/1/10**
DATE APPROVED BY NERC	**10/26/10**
DATE PROVIDED TO FERC	**10/26/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**8/26/10**
DATE OF CERTIFICATION LETTER	**1/6/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**8/26/10**
DATE OF VERIFICATION LETTER	**2/16/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**8/26/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
UREs reiterated to employees and contract workers the importance of strict compliance with the CIP Standards and coached pertinent personnel regarding CIP procedures. UREs revised its visitor procedure to expand descriptions of the responsibilities of escorts and visitors within restricted areas. URE 1 and URE 2 implemented a requirement that contract workers who regularly require access to a PSP undergo a PRA and cyber security training in order to gain authorized unescorted access to the necessary 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)

- **URE 2 memo to all Employees stressing the importance of adhering to the requirements of NERC CIP standards.**
- **URE 2 memo to all UREs NERC CIP cleared individuals (including contractors) regarding change to UREs' visitor procedure for NERC CIP areas.**
- **UREs provided photocopies of training records containing signatures of employees attending and the attendance date.**

- **UREs provided a copy of procedure for visitors within CIP restricted areas and logging.**
- **UREs provided a photocopy of an internal memo to subject employee. The memo summarizes a conversation between these parties, during which the subject employee was counseled on failure to adhere to UREs security procedure regarding escort of visitors into a Physical Security Perimeter.**
- **UREs provided a photocopy of an internal memo in which UREs agree that contract workers that regularly require access to PSP receive a PRA, cyber security training and authorized unescorted physical access.**

EXHIBITS:

SOURCE DOCUMENT
URE 1 and URE 2's Violation Self-Reporting Form for RFC201000228 and RFC201000231

URE 1 and URE 2's Violation Self-Reporting Form for RFC201000597 and RFC201000603

MITIGATION PLAN
URE 1 and URE 2's Mitigation Plans MIT-10-2429 and MIT-10-2438 for RFC201000228 and RFC201000231

URE 1 and URE 2's Mitigation Plans MIT-10-2915 for RFC201000597 and RFC201000603

CERTIFICATION BY REGISTERED ENTITY
URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000228 and RFC201000231

URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000597 and RFC201000603

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2429 and MIT-10-2438 for RFC201000228 and RFC201000231

Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2915 for RFC201000597 and RFC201000603

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment e-4

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000424: URE 1	**RFC201000424**
RFC201000425: URE 2	**RFC201000425**
RFC201000598: URE 1	**RFC201000598**
RFC201000599: URE 1	**RFC201000599**
RFC201000604: URE 2	**RFC201000604**
RFC201000605: URE 2	**RFC201000605**
RFC201000661: URE 1	**RFC201000661**

I. VIOLATION INFORMATION

VIOLATION ID	RELIABILITY STANDARD	REQUIREMENT (S)	SUB-REQUIREMENT(S)	VRF(S)	VSL (S)
RFC201000424	**CIP-007-1**	**6**		**Lower**[1]	**N/A**[2]
RFC201000425	**CIP-007-1**	**6**		**Lower**	**N/A**
RFC201000598	**CIP-007-2a**	**1**		**Lower**[3]	**Severe**[4]
RFC201000599	**CIP-007-2**[5]	**3**	**3.1**	**Lower**	**Severe**[6]
RFC201000604	**CIP-007-2a**	**1**		**Medium**	**Severe**
RFC201000605	**CIP-007-2**	**3**	**3.1**	**Lower**	**Severe**
RFC201000661	**CIP-007-2**	**5**	**5.2.3**	**Medium**[7]	**Moderate**

[1] CIP-007-1 R6, R6.4 and R6.5 are assigned Lower Violation Risk Factors (VRFs) and CIP-007-1 R6.1, R6.2 and R6.3 each are assigned a Medium VRF.
[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] CIP-007 R1 and R1.1 each have a Medium VRF; R1.2 and R1.3 each have a Lower VRF.
[4] 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 for RFC201000598, RFC201000599, RFC201000604, RFC201000605, and RFC201000661.
CIP-007-2a R1 only has an available VSL of Severe. Reliability*First* applied a VSL of High for the CIP-007-2a R1 violations prior to the January 20, 2011 FERC Order approving Version 2 VSLs.
[5] The language of CIP-007-1, R3.1 and CIP-007-2, R3.1 is the same. The duration of the RFC201000599 and RFC201000605 violations span both Version 1 and Version 2 of the Reliability Standard. Reliability*First* processed RFC201000599 and RFC201000605 as violations of Version 2.
[6] CIP-007-2 R3/3.1 only has an available VSL of Severe. Reliability*First* applied a VSL of High for the CIP-007-2a R3/3.1 violations prior to the January 20, 2011 FERC Order approving Version 2 VSLs.
[7] CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, R5.2.2, R5.3, R5.3.1 and R5.3.2 each have a Lower VRF; R5.1, R5.1.3, R5.2.1 and R5.2.3 each have a Medium VRF.

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

The purpose statement of CIP-007 provides: "Standard CIP-007 requires Responsible Entities[8] 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."[9] (Footnote added.)

CIP-007-1 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 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.**
>
> **R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.**

CIP-007-2 provides in pertinent part:

> **R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.**

[8] 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.

[9] The only change between the two versions of the Standard is that the Purpose Statement of Version Two of the Reliability Standard refers to CIP-007-2.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

****

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

****

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

****

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

****

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

(automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

VIOLATION DESCRIPTION

CIP-007-1 R6 (RFC201000424 and RFC201000425)[10]
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-007-1 R6. URE 1 and URE 2 discovered that some of their Cyber Assets located within an Electronic Security Perimeter (ESP) were not configured to send log information to a centralized location to enable it to be reviewed. Specifically, URE 1 and URE 2 failed to configure 44 Cyber Asset devices as required. Despite being incapable of sending log information to a centralized location for review, 23 of the 44 devices' logging capabilities were sufficient to capture at least 90 days of log data at all times. As a result, URE 1 and URE 2 later reviewed the logs of those 23 devices to confirm the lack of cyber security system events for the entire period. Regarding nine of the 44 devices, URE 1 and URE 2 were able to retrieve between six and 34 days of logs for each device, confirming the lack of cyber security system events for those days. Regarding an additional nine of the 44 devices, URE 1 and URE 2 retrieved at least 90 days of logs, but because the devices were overwritten, URE 1 and URE 2 were unable to review the logs for the existence of cyber security system events. Regarding the remaining three devices, URE 1 and URE 2 could retrieve no log information for the period between when URE 1 and URE 2 had to be compliant and the date of discovery. As a result, URE 1 and URE 2 could not review those logs for cyber security system events. URE 1 and URE 2 therefore failed to retain logs for 90 calendar days as required by CIP-007-1 R6.4, and failed to review the logs for the existence of cyber security system events, as required by CIP-007-1 R6.5.

CIP-007-2a R1 (RFC201000598 and RFC201000604)
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-007-2a R1. The information services department discovered that it failed to complete required cyber security testing when it installed new software. Although URE 1 and URE 2 have cyber security test procedures in place, the information services department mistakenly installed a new software onto four servers without testing whether this change would adversely affect existing cyber security controls.

CIP-007-2 R3.1 (RFC201000599 and RFC201000605)
URE 1 and URE 2 submitted a Self-Report to Reliability*First* identifying violations of CIP-007-2 R3.1. URE 1 and URE 2 discovered that they failed to timely assess security patches related to a software upgrade and URE 2 discovered that it failed to timely assess additional security patches. Specifically, the information services

[10] Some of the supporting documents refer to these violations as violations of the CIP-007-2aversion of the Reliability Standard.

department failed to assess a security-related software upgrade for URE 1 and URE 2. In addition, URE 2 miscalculated the due date for its assessment of several security patches, and it assessed those security patches at 31 calendar days, one day beyond the 30 days required by the Reliability Standard.

CIP-007-2 R5.2.3 (RFC201000661)
The violation of CIP-007-2 R5.2.3 is by URE 1 only. URE 1 submitted a Self-Report to Reliability*First* identifying a violation of CIP-007-2 R5.2.3. URE 1 discovered that the information services department did not timely revoke an individual's access to a shared account. URE 1 has a procedure in place for managing the use of shared accounts in which it specifies that URE 1 must revoke access to shared accounts within seven days of the date the employee no longer requires such access. An individual resigned from URE 1 on August 6, 2010, and according to its policy, URE 1 should have revoked access to the shared account on August 13, 2010. URE 1 failed to revoke the individual's access to a shared account until August 16, 2010, ten days after the individual no longer required access. URE 1 revoked this individual's physical and electronic access to its facilities and computer systems within the seven day period, as required by CIP-004.

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-007-1 R6 (RFC201000424 and RFC201000425)
The 44 devices at issue are located within an ESP that has access control and monitoring in place. Anti-virus systems protect all of the devices except three, for which URE 1 and URE 2 have a Technical Feasibility Exception (TFE).[11] These anti-virus systems would have alerted URE 1 and URE 2 of any malware-related cyber security system events. Strong two-factor electronic access controls, as well as account management controls, protect the devices as well. Furthermore, for all of the devices' logs that URE 1 and URE 2 retrieved and reviewed, they found no cyber security system events during the relevant time period. URE 1 and URE 2 also verified that their normal procedure for logging and review was functioning properly.

CIP-007-2a R1 (RFC201000598 and RFC201000604)
The servers at issue had other system security protections in place, such as compliant and secure account management controls, anti-malware protection, and security monitoring and logging protections that provide alerts when anomalous events occur. In addition, the information services department functionally tested the software on similar systems in May and June, 2010, reducing the risk that the

[11] Reliability*First* has accepted and approved both TFEs.

lack of testing on the four servers at issue would adversely affect existing cyber security controls.

CIP-007-2 R3.1 (RFC201000599 and RFC201000605)
The UREs' firewalls have very few ports and entry to those ports requires access from firewall administrators with elevated privileges. Furthermore, these firewalls are internally-facing, so they do not communicate outside the UREs' system. In addition, administrators with elevated privileges are the only individuals with access to the firewalls. These protections reduce the risk that the failure to assess security patches and upgrades would allow an unauthorized user to gain access to the UREs' system.

CIP-007-2 R5.2.3 (RFC201000661)
URE 1 revoked the individual's physical access to the building and the room containing the CCAs, so the individual could not have physically accessed the CCAs. Furthermore, URE 1 revoked the individual's unescorted physical access and electronic access to the UREs' computer network within the requisite time period. Since the individual never had remote cyber access to the CCAs, timely revocation of physical access effectively prevented all access to the CCAs. The individual did not re-enter the building as a visitor after resignation.

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-007-1 R6 (RFC201000424 and RFC201000425)
1/1/10 through 6/18/10 (when URE 1 and URE 2 remedied the assets' configurations)

CIP-007-2a R1 (RFC201000598 and RFC201000604)
6/21/10 through 6/30/10 (when URE 1 and URE 2 removed the software from the servers)

CIP-007-2 R3.1 (RFC201000599 and RFC201000605)
1/1/10 through 7/14/10 (when URE 1 and URE 2 assessed the security patches and upgrades)

CIP-007-2 R5.2.3 (RFC201000661)
8/31/10 (when the individual no longer required access to shared accounts) through 8/16/10 (when URE 1 revoked such access)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

CIP-007-1 R6 (RFC201000424 and RFC201000425) **Self-Report**

CIP-007-2a R1 (RFC201000598 and RFC201000604)
CIP-007-2 R3.1 (RFC201000599 and RFC201000605) **Self-Report**

CIP-007-2 R5.2.3 (RFC201000661) **Self-Report**

ARE THE VIOLATIONS STILL OCCURRING YES ☐ NO ☒
IF YES, EXPLAIN

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

III. MITIGATION INFORMATION

CIP-007-1 R6 (RFC201000424 and RFC201000425)
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2782 and MIT-10-2783**[12]
DATE SUBMITTED TO REGIONAL ENTITY	**7/30/10**
DATE ACCEPTED BY REGIONAL ENTITY	**8/10/10**[13]
DATE APPROVED BY NERC	**9/1/10**
DATE PROVIDED TO FERC	**9/1/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

[12] Though NERC assigned separate ID numbers for URE 1's and URE 2's Mitigation Plan, URE 1 and URE 2 submitted one Mitigation Plan.
[13] The Verification of Mitigation Plan Completion has a typographical error that states Reliability*First* accepted this Mitigation Plan on August 10, 2010.

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**6/18/10**
DATE OF CERTIFICATION LETTER	**1/6/11**[14]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**6/18/10**
DATE OF VERIFICATION LETTER	**2/3/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**6/18/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE 1 and URE 2 harvested all retrievable local device event, security, and application logs and reviewed them, finding no cyber security system events. In addition, URE 1 and URE 2 promptly remediated the configuration problems that caused the alleged violation by correctly configuring the devices to send their logs to the centralized location. URE 1 and URE 2 also implemented a network configuration manager for network infrastructure assets, which provides automated oversight ensuring the proper configuration of many of the affected assets. To oversee all of the affected assets, URE 1 and URE 2 installed additional software solutions. URE 1 and URE 2 also informed and instructed personnel about this incident and reiterated the importance of CIP compliance.

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)

- **Samples of daily reports from the new tool that was put into place to automate the management of the configuration of cyber assets for logging.**
- **Log device listing that lists the 32 cyber assets that have been remediated to send their logs to a centralized location for review.**

CIP-007-2a R1 (RFC201000598 and RFC201000604)

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2916**
DATE SUBMITTED TO REGIONAL ENTITY	**8/31/10**
DATE ACCEPTED BY REGIONAL ENTITY	**10/1/10**
DATE APPROVED BY NERC	**10/26/10**
DATE PROVIDED TO FERC	**10/26/10**

[14] The Verification of Mitigation Plan Completion has a typographical error that states URE submitted its Certification of Mitigation Plan completion on December 17, 2010.

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **7/2/10**

DATE OF CERTIFICATION LETTER **1/19/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **7/2/10**

DATE OF VERIFICATION LETTER **2/7/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **7/2/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
After discovering the improper installation, URE 1 and URE 2 removed the software from the four servers. URE 1 and URE 2 counseled the individuals responsible for installation regarding the importance of change management procedures, including cyber security testing protocols.

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)

- **Photocopy of a screenshot noting the software was removed from affected servers on June 30, 2010, dated June 30, 2010.**
- **Copy of memo attesting that he provided awareness and feedback to those involved and to ensure a clear understanding of the need to perform Cyber Security testing**

CIP-007-2 R3.1 (RFC201000599 and RFC201000605)
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **MIT-10-2917**
DATE SUBMITTED TO REGIONAL ENTITY **8/31/10**
DATE ACCEPTED BY REGIONAL ENTITY **10/1/10**
DATE APPROVED BY NERC **10/26/10**
DATE PROVIDED TO FERC **10/26/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**7/19/10**
DATE OF CERTIFICATION LETTER	**1/19/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**7/19/10**
DATE OF VERIFICATION LETTER	**2/7/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**7/19/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE 1 and URE 2 assessed the security patches and upgrades and counseled the individuals responsible for assessment to ensure that they carefully review patches and upgrades as well as the assessment due dates.
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)

- **Photocopy of an email memo attesting to having had conversations with the URE employee of note in the MP.**
- **Photocopy of a page for check point vulnerability**
- **Photocopy of an email attesting that the computer security patches were assessed**
- **Photocopy of an email to the involved employee of note in the MP. The memo summarizes a meeting with the involved employee during which the employee was counseled on the requirement of the CIP standard and the employee's responsibility to adhere to the language of the standard in the future.**

CIP-007-2 R5.2.3 (RFC201000661)
FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-3316**
DATE SUBMITTED TO REGIONAL ENTITY	**12/22/10**[15]
DATE ACCEPTED BY REGIONAL ENTITY	**1/27/11**
DATE APPROVED BY NERC	**2/23/11**
DATE PROVIDED TO FERC	**2/25/11**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE
On October 19, 2010, URE 1 had submitted this Mitigation Plan to correct the self-reported CIP-004-2 R4 violation. On December 22, 2010, URE 1 resubmitted this

[15] The Revised Mitigation Plan retained the October 19, 2010 date.

Mitigation Plan to correctly identify the Reliability Standard and Requirement as CIP-007-2 R5.2.3.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **10/8/10**

DATE OF CERTIFICATION LETTER **1/19/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **10/8/10**

DATE OF VERIFICATION LETTER **3/21/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **10/8/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE 1 changed the shared account password and removed the individual from the authorized access list. URE 1 also provided additional guidance to its personnel regarding access removals. In addition, URE 1 revised the password change procedure to reflect the access removal time window.

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)

- **E-Mail attestations of Mitigation Plan Evidence.**
- **Account and password procedure**

EXHIBITS:

SOURCE DOCUMENT
URE 1 and URE 2's Violation Self-Reporting Form for RFC201000424 and RFC201000425

URE 1 and URE 2's Violation Self-Reporting Form for RFC201000598 and RFC201000604

URE 1 and URE 2's Violation Self-Reporting Form for RFC201000599 and RFC201000605

URE 1's Violation Self-Reporting Form for RFC201000661

MITIGATION PLAN

URE 1 and URE 2's Mitigation Plans MIT-10-2782 and MIT-10-2783 for RFC201000424 and RFC201000425

URE 1 and URE 2's Mitigation Plans MIT-10-2916 for RFC201000598 and RFC201000604

URE 1 and URE 2's Mitigation Plans MIT-10-2917 for RFC201000599 and RFC201000605

URE 1 and URE 2's Mitigation Plans MIT-10-3316 for RFC201000661

CERTIFICATION BY REGISTERED ENTITY

URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000424 and RFC201000425

URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000598 and RFC201000604

URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000599 and RFC201000605

URE 1 and URE 2's Certification of Mitigation Plan Completion for RFC201000661 submitted January 19, 2011

VERIFICATION BY REGIONAL ENTITY

Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2782 and MIT-10-2783 for RFC201000424 and RFC201000425

Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2916 for RFC201000598 and RFC201000604

Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-2917 for RFC201000599 and RFC201000605

Reliability*First*'s Verification of Mitigation Plan Completion for MIT-10-3316 for RFC201000661