NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 30, 2011

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

Re: NERC Abbreviated Notice of Penalty regarding Unidentified Registered 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 (URE1), Unidentified Registered Entity 2 (URE2) and Unidentified Registered Entity 3 (URE3) (collectively, UREs), with information and details regarding the nature and resolution of the violation[1] discussed in detail in the Settlement Agreement (Attachment f) and the Disposition Documents (Attachment g), 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 enforceable violations of CIP-004-1 Requirement (R) 2.1, CIP-004-1 R3, CIP-002-1 R3.2, CIP-004-1 R4, and CIP-008-1 R1. According to the Settlement Agreement, the UREs admit to the violations and agree to the assessed penalty of fifty two thousand five hundred dollars ($52,500), in addition to other remedies and actions to mitigate the instant violations and facilitate future

[1] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.
[2] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2010). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers RFC200900129, RFC200900130, RFC200900191, RFC200900192, RFC200900193, RFC200900264, RFC200900265, RFC200900266, RFC200900267, RFC200900268, RFC200900269, RFC200900270, RFC200900271 and RFC200900272 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 September 10, 2010, 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	Registered Entity	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
NOC-684	URE1	RFC200900129	CIP-004-1	2.1	Medium[3]	1/29/09-6/5/09	$52,500
	URE2	RFC200900130	CIP-004-1	2.1	Medium[4]	1/29/09-6/5/09	
	URE1	RFC200900191	CIP-004-1	3	Medium[5]	8/7/09-9/8/09	
	URE3	RFC200900192	CIP-004-1	3	Medium[6]	8/7/09-9/8/09	
	URE2	RFC200900193	CIP-004-1	3	Medium[7]	8/7/09-9/8/09	

[3] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" Violation Risk Factor (VRF); R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective. The Settlement Agreement at P. 30 incorrectly states R2.1 had a "Lower" VRF at the time of the violation.

[4] *Id*.

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

[6] *Id*.

[7] *Id*.

NOC ID	Registered Entity	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
	URE1	RFC200900264	CIP-002-1	3.2	Lower[8]	6/30/09-12/17/09	
	URE1	RFC200900265	CIP-004-1	4	Lower	8/29/08-7/1/09	
	URE1	RFC200900266	CIP-008-1	1[9]	Lower	7/1/08-10/28/09	
	URE2	RFC200900267	CIP-002-1	3.2	Lower[10]	6/30/09-12/17/09	
	URE2	RFC200900268	CIP-004-1	4	Lower	8/29/08-7/1/09	
	URE2	RFC200900269	CIP-008-1	1[11]	Lower	7/1/08-10/28/09	
	URE3	RFC200900270	CIP-002-1	3.2	Lower[12]	6/30/09-12/17/09	
	URE3	RFC200900271	CIP-004-1	4	Lower	8/29/08-7/1/09	
	URE3	RFC200900272	CIP-008-1	1[13]	Lower	7/1/08-10/28/09	

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

CIP-004-1 R2.1 - OVERVIEW

On April 24, 2009, URE1 and URE2 submitted a Self-Report to Reliability*First* for two violations of CIP-004-1 R2.1. Reliability*First* determined that URE1 and URE2 failed to train three contractors with authorized unescorted physical access to Critical Cyber Assets.

CIP-004-1 R3 - OVERVIEW

On October 5, 2009, the UREs submitted Self-Reports to Reliability*First* for three violations of CIP-004-1 R3. Reliability*First* determined that the UREs failed to ensure that personnel risk assessments were conducted within 30 days of certain contracted workers and employees being granted authorized unescorted physical access to Critical Cyber Assets.

[8] CIP-002-1 R3 has a "High" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 a "Medium" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "High" VRF and on January 27, 2009, the Commission approved the modified "High" VRF. Therefore, the" Medium" VRF for CIP-002-1 R3 was in effect from June 18, 2007 until January 27, 2009, when the "High" VRF became effective.

[9] In the context of this case, Reliability*First* determined the CIP-008-1 R1 violation related to both R1.1 and R1.4. The Settlement Agreement at P. 39 incorrectly states the violation was related to R1.6.

[10] *See* n. 8.

[11] *See* n. 9.

[12] *See* n. 8.

[13] *See* n. 9.

CIP-002-1 R3.2 - OVERVIEW

During a Spot Check, Reliability*First* discovered three violations of CIP-002-1 R3.2. Reliability*First* determined that the UREs improperly removed thirteen operator consoles from their lists of Critical Cyber Assets because of a mistaken belief that operator consoles, individually, were not essential to the operation of the Critical Assets and therefore could be considered non-critical.

CIP-004-1 R4 - OVERVIEW

During the Spot Check, Reliability*First* discovered three violations of CIP-004-1 R4. Reliability*First* determined that the UREs failed to maintain lists of its personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including specific electronic and physical access rights to Critical Cyber Assets.

CIP-008-1 R1 - OVERVIEW

During the Spot Check, Reliability*First* discovered three violations of CIP-008-1 R1. Reliability*First* determined that the UREs failed to develop and maintain Cyber Security Incident response plans that addressed (a) procedures for characterizing and classifying events as reportable Cyber Security Incidents, as required by R1.1; and (b) a process for updating the plan within 90 calendar days of any changes, as required by R1.4.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[14]

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,[15] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2010. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of a fifty two thousand five hundred dollar ($52,500) 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 violations constituted the UREs' first violation of the subject NERC Reliability Standards;
2. the UREs self-reported the CIP-004-1 R2.1 and R3 violations, while the other violations were discovered in the Spot Check;

[14] *See* 18 C.F.R. § 39.7(d)(4).

[15] *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).

3. Reliability*First* reported that the UREs were cooperative throughout the compliance enforcement process;
4. the UREs had a compliance program at the time of the violations, which Reliability*First* considered a mitigating factor, as discussed in the Disposition Documents;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. Reliability*First* determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), as discussed in the Disposition Documents;
7. Reliability*First* found that the mitigation plan addressing the violations of CIP-004-1, R3 was scheduled to be completed on December 18, 2009 but was not completed until March 16, 2010; and
8. 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. The NERC BOTCC believes that the assessed penalty of fifty two thousand five hundred dollars ($52,500) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

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

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

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

Attachments to be included as Part of this Notice of Penalty

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

a) URE1 and URE2's Self-Reports for CIP-004-1 R2.1 dated April 24, 2009, included as Attachment a;

b) UREs' Self-Reports for CIP-004-1 R3 dated October 5, 2009, included as Attachment b;

c) Reliability*First*'s Summary for a Possible Violation of CIP-002-1 R3.2, included as Attachment c;

d) Reliability*First*'s Summary for a Possible Violation of CIP-004-1 R4, included as Attachment d;

e) Reliability*First*'s Summary for a Possible Violation of CIP-008-1 R1, included as Attachment e;

f) Settlement Agreement by and between Reliability*First* and the UREs executed September 10, 2010, included as Attachment f;

   i. UREs' Mitigation Plan MIT-08-2537 for CIP-002-1 R3.2 and Certification of Mitigation Plan Completion included therein submitted April 30, 2010, included as Attachment A to the Settlement Agreement;

   ii. Reliability*First*'s Verification of Mitigation Plan MIT-08-2537 Completion for CIP-002-1 R3.2 dated August 11, 2010, included as Attachment B to the Settlement Agreement;

   iii. URE1's Mitigation Plan MIT-08-1767 for CIP-004-1 R2.1 and Certification of Mitigation Plan Completion included therein submitted June 18, 2009, included as Attachment C to the Settlement Agreement;

   iv. URE2's Mitigation Plan MIT-08-1768 for CIP-004-1 R2.1 and Certification of Mitigation Plan Completion included therein submitted June 18, 2009, included as Attachment D to the Settlement Agreement;

   v. Reliability*First*'s Verifications of Mitigation Plan MIT-08-1767 and MIT-08-1768 Completion for CIP-004-1 R2.1 both dated September 4, 2009, included as Attachment E to the Settlement Agreement;

   vi. UREs' Mitigation Plan MIT-08-2186 for CIP-004-1 R3 submitted November 24, 2009, included as Attachment F to the Settlement Agreement;

   vii. UREs' Certification of Mitigation Plan MIT-08-2186 Completion for CIP-004-1 R3 dated March 18, 2010, included as Attachment G to the Settlement Agreement

   viii. Reliability*First*'s Verification of Mitigation Plan MIT-08-2186 Completion for CIP-004-1 R3 dated March 31, 2010, included as Attachment H to the Settlement Agreement;

   ix. UREs' revised Mitigation Plan MIT-08-2781 for CIP-004-1 R4 submitted July 27, 2010, included as Attachment I to the Settlement Agreement;

x. UREs' Mitigation Plan MIT-09-2538 for CIP-008-1 R1 and Certification of Mitigation Plan Completion included therein submitted April 30, 2010, included as Attachment J to the Settlement Agreement;

xi. Reliability*First*'s Verification of Mitigation Plan MIT-09-2538 Completion for CIP-008-1 R1 dated August 11, 2010, included as Attachment K to the Settlement Agreement;

g) Disposition Document for Common Information dated December 10, 2010, included as Attachment g:

i. Disposition Document for CIP-004-1 R2.1, included as Attachment g-1;

ii. Disposition Document for CIP-004-1 R3, included as Attachment g-2;

iii. Disposition Document for CIP-002-1 R3.2, included as Attachment g-3;

iv. Disposition Document for CIP-004-1 R4, included as Attachment g-4;

v. Disposition Document for CIP-008-1 R1, included as Attachment g-5;

h) UREs' Certification of Mitigation Plan MIT-08-2781 Completion for CIP-004-1 R4 dated December 21, 2009, included as Attachment h; and

i) Reliability*First*'s Verification of Mitigation Plan MIT-08-2781 Completion for CIP-004-1 R4 dated February 9, 2011, included as Attachment i.

A Form of Notice Suitable for Publication[16]

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

[16] *See* 18 C.F.R. § 39.7(d)(6).

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net Robert K. Wargo* Manager of Compliance Enforcement Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 bob.wargo@rfirst.org L. Jason Blake* Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 jason.blake@rfirst.org Michael D. Austin* Associate Attorney 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 mike.austin@rfirst.org

Conclusion

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

Respectfully submitted,

/s/ *Rebecca J. Michael*
Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Sonia C. Mendonça*
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

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

cc: Unidentified Registered Entities
ReliabilityFirst Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment g

Disposition Document for Common Information dated December 10, 2010

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS
Dated December 10, 2010

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity 1 (URE1)	**NCRXXXX1**	**NOC-684**
Unidentified Registered Entity 2 (URE2)	**NCRXXXX2**	
Unidentified Registered Entity 3 (URE3)	**NCRXXXX3**	

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	☒[2]
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 **$52,500** FOR **FOURTEEN** VIOLATIONS OF RELIABILITY STANDARDS.

[1] For purposes of this document and attachments hereto, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.
[2] The UREs stipulate that the facts outlined in the Settlement Agreement constitute violations of ClP-002-1 R3.2; CIP-004-1 R2.1, R3, and R4; and ClP-008-1 R1.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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
The UREs had a documented compliance program in place at the time of the violations that Reliability*First* considered a mitigating factor in determining the penalty.

EXPLAIN SENIOR MANAGEMENT'S ROLE AND INVOLVEMENT WITH RESPECT TO THE REGISTERED ENTITY'S COMPLIANCE PROGRAM, INCLUDING WHETHER SENIOR MANAGEMENT TAKES ACTIONS THAT SUPPORT THE COMPLIANCE PROGRAM, SUCH AS TRAINING, COMPLIANCE AS A FACTOR IN EMPLOYEE EVALUATIONS, OR OTHERWISE.

(4) ANY ATTEMPT BY THE REGISTERED ENTITY TO CONCEAL THE VIOLATION(S) OR INFORMATION NEEDED TO REVIEW, EVALUATE OR INVESTIGATE THE VIOLATION.

YES ☐ NO ☒
IF YES, EXPLAIN

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

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☒ NO ☐
IF YES, EXPLAIN
Reliability*First* considered that the mitigation plan addressing the violations of CIP-004-1, R3 was scheduled to be completed on December 18, 2009 but was not actually completed until March 16, 2010.

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

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

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **8/31/09**[3] OR N/A ☐

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

SUPPLEMENTAL RECORD INFORMATION
DATE(S) OR N/A ☒

REGISTERED ENTITY RESPONSE CONTESTED
FINDINGS ☐ PENALTY ☐ BOTH ☐ NO CONTEST ☒

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

[3] Settlement discussions commenced on August 31, 2009 for RFC200900129 and RFC200900130 and on February 12, 2010 for RFC200900191, RFC200900192 and RFC200900193. Settlement discussions commenced for the remainder of the violations on March 26, 2010.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-1 R2.1

DISPOSITION OF VIOLATION
Dated December 10, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC200900129	**RFC200900129**
RFC200900130	**RFC200900130**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**2**	**2.1**	**Medium**[1]	**N/A**[2]

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

The purpose statement of CIP-004-1 provides in pertinent part: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.…"
CIP-004-1 R2 provides:

> **R2. Training — The Responsible Entity[3] shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary. (Footnote added.)**

[1] The Settlement Agreement at P 30 provided that R2.1 had a "Lower" VRF at the time of the violation. CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" Violation Risk Factor (VRF); R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. The Commission approved the VRF as filed, but it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[2] At the time of the violations, Violation Severity Levels (VSLs) were not in effect for CIP-004-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[3] Within the text of Standard CIP-004, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC and Regional Reliability Organizations.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

VIOLATION DESCRIPTION

On April 24, 2009, URE1 and URE2 submitted a Self-Report to Reliability*First* for two violations of CIP-004-1 R2.1. Three[4] contractors performing work for URE1 and URE2 had authorized unescorted physical access to Critical Cyber Assets. These contractors, however, did not complete cyber security training within ninety days of being authorized to work in the Backup Control Room and Backup Server Room.

The three contractors were authorized to have unescorted physical access to URE1 and URE2's shared Backup Control Room, and Backup Server Room. Collectively, the three contractors accessed these two locations six times to work on security equipment located in these rooms.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the CIP-004-1 R2.1 violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because these violations involved only three of the 199 URE1 and URE2 contractors with authorized cyber or authorized unescorted physical access to Critical Cyber Assets. Immediately upon learning that the individuals did not have the required training, URE1 and URE2 removed their access privileges until they received the required training. Before the violation occurred, URE1 and URE2 had performed personnel risk assessments on the subject individuals, which identified no issues.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

[4] The mitigation plan incorrectly refers to 16 contractors.

DURATION DATE(S) **1/29/09 (ninety days after the contractors were first granted access to Critical Cyber Assets) through 6/5/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **4/24/09**

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:
MITIGATION PLAN NO. **MIT-08-1767 (RFC200900129) and MIT-08-1768 (RFC200900130)**
DATE SUBMITTED TO REGIONAL ENTITY **6/18/09**
DATE ACCEPTED BY REGIONAL ENTITY **6/24/09**
DATE APPROVED BY NERC **6/29/09**
DATE PROVIDED TO FERC **6/29/09**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **6/5/09**

DATE OF CERTIFICATION LETTER **6/18/09**[5]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **6/5/09**

DATE OF VERIFICATION LETTER **9/4/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **6/5/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
URE1 and URE2 performed a complete review of existing personnel with authorized cyber or authorized unescorted physical access to Critical Cyber

[5] URE1 and URE2's Certifications of Mitigation Plan completion were included in the Mitigation Plans.

Assets and verified and ensured that those personnel have undergone training.

URE1 revised its internal access control policy to require training before access is granted. URE2 was required to follow this policy.

URE1 revised its internal procedure for Critical Cyber Asset access review to require a quarterly review of the training status of each person granted access. URE2 was required to follow this policy.

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)
The access control policy is an internal procedure which governs issuance of access control devices to personnel. The policy requires completion of cyber security training prior to issuance of an access control device.

The Critical Cyber Asset access review policy is an internal process which governs the quarterly review of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The policy requires a review to validate that all personnel with access to Critical Assets have completed required training.

EXHIBITS:

SOURCE DOCUMENT
URE1 and URE2's Self-Report for CIP-004-1 R2.1 dated April 24, 2009

MITIGATION PLAN AND CERTIFICATION BY REGISTERED ENTITY
URE1's Mitigation Plan MIT-08-1767 for CIP-004-1 R2.1 and Certification of Mitigation Plan Completion included therein submitted June 18, 2009

URE2's Mitigation Plan MIT-08-1768 for CIP-004-1 R2.1 and Certification of Mitigation Plan Completion included therein submitted June 18, 2009

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verifications of Mitigation Plan MIT-08-1767 and MIT-08-1768 Completion for CIP-004-1 R2.1 both dated September 4, 2009

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-1 R3

DISPOSITION OF VIOLATION
Dated December 10, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC200900191	**RFC200900191**
RFC200900192	**RFC200900192**
RFC200900193	**RFC200900193**

I. VIOLATION INFORMATION

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

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

The purpose statement of CIP-004-1 provides in pertinent part: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.…"

CIP-004-1 R3 provides:

> **R3. Personnel Risk Assessment —The Responsible Entity[3] shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A**

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

[2] At the time of the violation, no VSLs were in effect for CIP-004-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[3] Within the text of Standard CIP-004, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC and Regional Reliability Organizations.

personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

R3.1. 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.

(Footnote added.)

VIOLATION DESCRIPTION

On October 5, 2009, the UREs submitted three separate Self-Reports to Reliability*First* for violation of CIP-004-1 R3. During an internal review of records related to personnel risk assessments (PRAs) for contractors with access to Critical Cyber Assets, the UREs found that there were: (1) two contractors for whom a PRA was not conducted by their employers and (2) an additional contractor whose employer represented to the UREs that it had conducted a PRA but upon review could not produce written records demonstrating the PRA was performed. [4]

When it was determined that PRA documentation could not be produced by the employers, access was immediately removed for the three (two without PRA reviews

[4] URE1 and URE2's October 5, 2009 Self-Reports each identified 14 contracted workers for whom no record of a PRA existed. Eleven (11) of those contracted workers were self-reported pursuant to the Transmission Owner function, a function that was not subject to compliance with CIP-004-1 until December 31, 2009. Therefore, those eleven (11) contracted workers were not included in this violation. URE1 ran physical access reports for the previous 90 days for the 14 contractors and found a total of five occasions where one of these contractors had entered the Physical Security Perimeter for a critical cyber asset. Additionally, upon discovery of the missing PRA documentation, the access was immediately removed for the contractors and PRAs performed for all 14 contractors. No irregularities were found in any of the PRAs.

and one without supporting PRA documentation) contractors until PRAs were performed.[5]

The three contractors were authorized to have unescorted access to the Server Room, but only one of them actually accessed the room during the 90 days for which the UREs had access records. The contractor accessed the Server Room on three different occasions in order to work on video equipment in the Server Room that is utilized by the operations control room displays, two of those occasions occurred within a single two-minute time span.

While mitigating the violation, the UREs reviewed the PRAs for the UREs employees, and discovered that two of the three employees with unescorted physical access to Critical Cyber Assets had PRAs in their files, but the PRAs were completed more than seven years ago. At the time of discovery, one employee was 34 days past seven years and, based on a review of previous 90 days access records, had no occasions of access to Critical Assets. The other employee was 137 days past seven years and, based on a review of previous 90 days access records, had 85 occasions of access to Critical Cyber Assets.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that these violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because a review of the previous 90 days of access records showed the locations accessed by the three contractors had a variety of security measures in place, including cameras, to track and record the movements of individuals.

For the two UREs employees with PRAs past seven years, a review of the previous 90 days of access indicates that one of those two employees had no instances of access. The other employee had 85 instances of access to the operations control room. The majority of these incidents occurred when the employee attended a daily work scheduling meeting within the operations control room. Because the operations control room is staffed 24 x 7, at no time during any of these instances would the employee have had unobserved or unmonitored access to any of the operations control room facilities.

[5] The narrative portion of the self-report incorrectly states that access was immediately removed for two contractors. The table shows that it was immediately removed for all three contractors.

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) **7/31/2008 to 9/8/2009 for two contractors and 8/6/2009 to 9/8/2009 for one contractor, which correspond to 30 days after which the first access was granted when the access was removed.**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **10/5/09**

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **MIT-08-2186**
DATE SUBMITTED TO REGIONAL ENTITY **11/24/09**
DATE ACCEPTED BY REGIONAL ENTITY **12/17/09**
DATE APPROVED BY NERC **1/12/10**
DATE PROVIDED TO FERC **1/12/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **12/18/2009**
EXTENSIONS GRANTED[6]
ACTUAL COMPLETION DATE **3/16/2010**

[6] The UREs did not submit a Mitigation Plan extension request. Reliability*First* took into consideration that the UREs did not complete the Mitigation Plan in the time period specified in that plan.

DATE OF CERTIFICATION LETTER **3/18/10 (signed 3/17/10)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **3/16/10**

DATE OF VERIFICATION LETTER **3/31/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **3/16/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE[7]

Access was immediately removed for the three contractors until PRAs were performed.

The UREs received and reviewed redacted copies of PRAs from the contractor's employers and conducted random on-site audits of the PRA records for a sample of contractors at their employers' location. This verification process included validating that the PRA consisted of at least identity verification and a seven-year criminal history check.

The UREs performed a review of PRAs for their employees and developed a spreadsheet to track the dates when PRAs were completed. As noted above, the UREs discovered that two of the three employees with unescorted physical access to Critical Assets had PRAs in their files, but were completed more than seven years ago.

In addition, the UREs reviewed and updated their personnel risk assessment policy to ensure that it was clear the criminal history check must go back at least seven years and be performed at least every seven years.

The UREs implemented spreadsheets to track the dates when PRAs were completed for every one of their employees and every contractor who has been given access to a Critical Asset or Critical Cyber Asset. The UREs also maintain a spreadsheet with all of the dates when these same employees and contractors last completed their annual cyber security training. As a next step, the UREs intend to merge these spreadsheets so that the PRA dates and training dates are tracked and maintained in one master document accessible to all individuals responsible for access control.

[7] Subsequent to its submittal of the Mitigation Plan, URE1 made additional changes to improve its process for contractor PRAs. URE1 modified the form that must be completed by the contract company attesting to the fact that the background check was completed. This form now requires the date the background check was completed. Additionally, URE1 now requires the contractor to submit a copy of the background check cover sheet or to submit a random audit of background check records on any of its employees with unescorted physical access to Critical Cyber Assets.

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)

URE1, URE2 and URE3 submitted the background check documents which included verification of PRAs being completed for three of the fourteen contractors listed in the Self-Reports. The UREs also provided evidence showing that the UREs verified PRAs were being completed for the remaining eleven of fourteen contractors.

After URE1, URE2 and URE3 completed a review of all remaining contractor PRA records and all URE1, URE2 and URE3 employee PRA records, it was discovered there were two employees whose PRAs were not completed in the last seven years. URE1, URE2, and URE3 provided evidence that these PRAs were conducted on November 19, 2009 and November 22, 2009.

URE1, URE2 and URE3 also supplied their master spreadsheet for tracking PRA and training records. This document showed that all PRAs were completed in the last seven years for all personnel who had access rights.

URE1, URE2 and URE3 submitted the personnel risk assessment policy as evidence that the document was updated on October 28, 2009 as per the Mitigation Plan. The update made it clear that the background check was to go back at least seven years and be performed again at least every seven years.

EXHIBITS:

SOURCE DOCUMENT
UREs' Self-Reports for CIP-004-1 R3 dated October 5, 2009

MITIGATION PLAN
UREs' Mitigation Plan MIT-08-2186 for CIP-004-1 R3 submitted November 24, 2009

CERTIFICATION BY REGISTERED ENTITY
UREs' Certification of Mitigation Plan MIT-08-2186 Completion for CIP-004-1 R3 dated March 18, 2010

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan MIT-08-2186 Completion for CIP-004-1 R3 dated March 31, 2010

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-002-1 R3.2

DISPOSITION OF VIOLATION
Dated December 10, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC200900264	**RFC200900264**
RFC200900267	**RFC200900267**
RFC200900270	**RFC200900270**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-002-1	**3**	**3.2**	**Lower**[1]	**N/A**[2]

PURPOSE OF THE RELIABILITY STANDARD AND TEXT OF RELIABILITY STANDARD AND REQUIREMENT(S)/SUB-REQUIREMENT(S)
The purpose statement of CIP-002-1 provides in pertinent part:

> **Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.**
>
> **Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.**
>
> **CIP-002-1 R3 provides:**
>
> **R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity[3]**

[1] CIP-002-1 R3 has a "High" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 a "Medium" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "High" VRF and on January 27, 2009, the Commission approved the modified "High" VRF. Therefore, the" Medium" VRF for CIP-002-1 R3 was in effect from June 18, 2007 until January 27, 2009, when the "High" VRF became effective.

[2] At the time of the violation, no VSLs were in effect for CIP-002-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[3] Within the text of Standard CIP-002, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission

shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

(Footnote added.)

VIOLATION DESCRIPTION

During a Spot Check of the UREs, Reliability*First* discovered three violations of CIP-002-1 R3.2. To determine compliance with CIP-002-1 R3, a list of Critical Cyber Assets associated with the UREs operations control room was reviewed. The operator consoles located in the operations control room were identified on the Critical Cyber Asset list that was in effect from June 30, 2008 until June 29, 2009. On June 30, 2009, 13 operator consoles were removed from the list of Critical Cyber Assets during the annual update process, based on a mistaken belief that operator consoles, individually, were not essential to the operation of the Critical Asset and therefore could be considered non-critical. At that time, the UREs did not believe the consoles met the evaluation criteria because the console functionality could easily be reestablished at a variety of other consoles that were available. The operator consoles provide monitoring and control of the bulk power system (BPS), Reliability*First* considered the consoles to be essential to the operation of the Critical Asset (operations control room) regardless of the availability of backup consoles.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that these violations did not pose a serious or substantial risk to the BPS because although the UREs did not list these operator consoles on its list of Critical Cyber Assets, it afforded these operator consoles all the protections

---

Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC and Regional Reliability Organizations.

afforded to Critical Cyber Assets, including locating them in an Electronic Security Perimeter and a Physical Security Perimeter.

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) **6/30/09 (the date on which the UREs removed the operator consoles from their list of Critical Cyber Assets) through 12/17/09 (Mitigation Plan completed)**

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-2537**[4]
DATE SUBMITTED TO REGIONAL ENTITY	**4/30/10**
DATE ACCEPTED BY REGIONAL ENTITY	**5/21/10**
DATE APPROVED BY NERC	**6/14/10**
DATE PROVIDED TO FERC	**6/14/10**

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

[4] The Settlement Agreement incorrectly states the Mitigation Plan for the CIP-002-1 R3.2 violations is designated MIT-09-2537.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **12/17/10**

DATE OF CERTIFICATION LETTER **4/30/10**[5]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **12/17/10**

DATE OF VERIFICATION LETTER **8/11/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **12/17/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
The UREs amended their Critical Cyber Asset list to once again include the operator consoles. As a result of the information communicated during the Spot Check, the UREs now have an enhanced understanding of the evaluation expectations and the addition of the operator consoles to the Critical Cyber Asset list will ensure their continued treatment as Critical Cyber Assets.

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)
During the Spot Check, Reliability*First* found evidence of how the UREs determined which of their Cyber Assets were deemed to be Critical Cyber Assets. The result of this process was documented. Reliability*First* determined that the consoles were on the list dated March 3, 2009, and were removed on June 30, 2009.

The UREs submitted a document that contains the list of Critical Cyber Assets essential to the operation of the UREs Critical Assets and now contained the operator consoles located in the operations control room.

[5] The Certification of Mitigation Plan completion was included in the Mitigation Plan.

EXHIBITS:

SOURCE DOCUMENT
Reliability*First*'s Summary for Possible Violation of CIP-002-1 R3.2

MITIGATION PLAN AND CERTIFICATION BY REGISTERED ENTITY
UREs' Mitigation Plan MIT-08-2537 for CIP-002-1 R3.2 and Certification of Mitigation Plan Completion included therein submitted April 30, 2010

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan MIT-08-2537 Completion for CIP-002-1 R3.2 dated August 11, 2010

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-1 R4

DISPOSITION OF VIOLATION
Dated December 10, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC200900265	**RFC200900265**
RFC200900268	**RFC200900268**
RFC200900271	**RFC200900271**

I. VIOLATION INFORMATION

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

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

The purpose statement of CIP-004-1 provides in pertinent part: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."

CIP-004-1 R4 provides:

> **R4. Access — The Responsible Entity[2] 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**

[1] At the time of the violation, no VSLs were in effect for CIP-004-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[2] 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.

Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

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

VIOLATION DESCRIPTION

During a Spot Check of the UREs, Reliability*First* discovered three violations of CIP-004-1 R4. Specifically, Reliability*First* reviewed the UREs' employee and contractor access lists for accuracy and to determine if appropriate approvals existed for the UREs' employees and contractors with access to Critical Cyber Assets. Reliability*First* found one employee had authorized unescorted physical access to two Critical Cyber Assets for which no record of authorization could be found prior to being added to the access lists maintained pursuant to CIP-004-1 R4. The employee in question had authorized unescorted physical access to other Critical Cyber Assets for which accesses were properly documented.[3]

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that these violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the subject individual had undergone cyber security training and a personnel risk assessment. This individual also had access to other Critical Cyber Assets, which was properly approved and documented in the UREs' list of individuals with access to Critical Cyber Assets.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

[3] The UREs were not able to determine whether the employee actually accessed the areas containing the two Critical Cyber Assets during the period for which he did not have documented access because by the time the alleged violation was identified, the employee was approved for access and the undocumented period was beyond the 90 day data retention period for access records.

DURATION DATE(S) **8/29/08 (the date on which the individual was granted access to the first Critical Cyber Asset) through 7/1/09 (when access to the second Critical Cyber Asset was reviewed and approved)**

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

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:
MITIGATION PLAN NO. **MIT-08-2781**[4]
DATE SUBMITTED TO REGIONAL ENTITY **7/27/10**
DATE ACCEPTED BY REGIONAL ENTITY **8/10/10**
DATE APPROVED BY NERC **10/27/10**[5]
DATE PROVIDED TO FERC **10/27/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **12/31/10**
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE **12/21/10**

DATE OF CERTIFICATION LETTER **12/21/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **12/21/10**

DATE OF VERIFICATION LETTER **2/9/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **12/21/10**

[4] A proposed Mitigation Plan for the CIP-004-1 R4 violations was submitted to Reliability*First* on April 30, 2010 with a proposed completion date of July 30, 2010. Reliability*First* never accepted this draft Mitigation Plan, but Reliability*First* inadvertently submitted this proposed Mitigation Plan to NERC which NERC approved on September 1, 2010 and was submitted as non-public information to FERC on September 1, 2010 in accordance with FERC orders. On July 27, 2010 the UREs submitted an additional draft Mitigation Plan that Reliability*First* ultimately accepted, in which it extended the approved completion date of July 30, 2010 to December 31, 2010. The UREs added an additional preventative milestone "to implement tracking of electronic access approvals in the new tool."
[5] The Verification of Mitigation Plan Completion incorrectly states that NERC approved the Mitigation Plan on September 1, 2010

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

The specific issue with the authorization record for the individual was addressed on December 3, 2009 by reviewing this employee's need for access and verifying that he showed up on a subsequent quarterly access list authorizing his physical access to the Critical Cyber Asset.

The UREs hired additional staff to help with their ongoing CIP compliance efforts as of March 31, 2010. A new position was created that is primarily focused on administering the physical access control system and associated recordkeeping. The new position receives and processes requests for new physical access and changes to physical access levels. When the request is received, the new position works with the UREs' human resources department, training department and the requestor to make sure that the individual has received a proper background check, has completed the cyber security training and that the appropriate sign offs from the access controllers have been obtained prior to granting the physical access. The new position is also responsible for maintaining all of these records in a file where they are accessible by the rest of the security department for review.

The UREs developed and implemented an electronic tool for the tracking of requests for both physical and electronic. This tool handles electronic signatures by multiple approvers including the appropriate access controllers and provides the ability to better track when these approvals were granted for future reviews and audits. In addition to providing a record of when access was approved, the tool also includes signoffs and completion dates for background checks and cyber security training. The tool does not allow the request to proceed to the implementer of the access until signoffs are completed by the appropriate approvers of the access, the verifier of the background check and verifier of the cyber security training. The system then stores all of the information pertaining to the approvals and the dates of the approvals, background checks and cyber security training. It immediately generates alerts if any individuals are granted access without the appropriate approvals within the system. It is also able to generate reports of all the individuals who do not have background checks or cyber security training records within the system and generate reports when any individual's background check or cyber security training is in need of renewal.

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)

- **The UREs submitted a job description for the new position described in the Mitigation Plan. The new position is responsible for implementing the UREs' access management programs.**
- **The UREs also provided an affidavit stating that they filled the new position.**
- **The UREs submitted two presentations showing evidence of training.**
  - **The UREs use both presentations to train users and approvers on the UREs' new electronic access tracking tool for authorized unescorted physical and electronic access to Critical Cyber Assets. These presentations also contain screenshots evidencing the development and implementation of this new tracking tool.**
  - **This tracking tool is used for all access changes and to verify access privileges match what has been approved. It also triggers notices when training and PRA records must be updated. The tool has built in workflow that handles approvals electronically. Each step of the workflow must be completed, before it goes to the next step, for example, a PRA and training must be completed, before going to an approver. The tracking tool stores all information pertaining to each step of the workflow for better tracking of access changes and approvals.**

EXHIBITS:

SOURCE DOCUMENT
Reliability*First*'s Summary for Possible Violations of CIP-004-1 R4

MITIGATION PLAN
UREs' Mitigation Plan MIT-08-2781 for CIP-004-1 R4 submitted July 27, 2010

CERTIFICATION BY REGISTERED ENTITY
UREs' Certification of Completion of Mitigation Plan MIT-08-2781 for CIP-004-1 R4 submitted December 21, 2010

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Completion of Mitigation Plan MIT-08-2781 for CIP-004-1 R4 submitted February 9, 2011

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-008-1 R1

DISPOSITION OF VIOLATION
Dated December 10, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC200900266	**RFC200900266**
RFC200900269	**RFC200900269**
RFC200900272	**RFC200900272**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-008-1	**1**	**1.1,1.4**[1]	**Lower**	**N/A**[2]

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

The purpose statement of CIP-008-1 provides: "Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009...."

CIP-008-1 R1 provides in pertinent part:

> **R1. Cyber Security Incident Response Plan — The Responsible Entity[3] shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident response plan shall address, at a minimum, the following:**
>
> **R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.**
>
> **…**

[1] In the context of this case, Reliability*First* determined the CIP-008-1 R1 violations related to both R1.1 and R1.4. The Settlement Agreement at P. 39 incorrectly states the violations were related to R1.6.

[2] At the time of the violation, no VSLs were in effect for CIP-008-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[3] Within the text of Standard CIP-008, "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.

R1.4. Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.

…

(Footnotes added.)

VIOLATION DESCRIPTION

During a Spot Check of the UREs, Reliability*First* discovered three violations of CIP-008-1 R1. Specifically, Reliability*First* reviewed all versions of the UREs' Cyber Security Incident response plan in effect prior to July 1, 2008 when the UREs were required to have such a plan. An earlier version of the Cyber Security Incident response plan did not include adequate procedures for characterizing and classifying events as reportable Cyber Security Incidents, as required by R1.1, nor a process for updating the plan within 90 calendar days of any changes, as required by R1.4.

Reliability*First* determined that a subsequent version of UREs' Cyber Security Incident response plan did include an adequate procedure to characterize and classify events as reportable Cyber Security Incidents as required by R1.1. Reliability*First* also determined that, although these versions of the response plans were not compliant with R1.4, a later version of UREs' Cyber Security Incident response plan included the requirement for updating the response plan within 90 calendar days of any changes as required by R1.4.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violations did not pose a serious or substantial risk to the bulk power system (BPS) because although the UREs' Cyber Security Incident Response Plan lacked certain required elements, the existence of this plan, especially the fact that it addressed the actions that the UREs would take in response to a Cyber Security Incident, mitigates the risk of this violation.

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) **7/1/08 (when the Standard became mandatory and enforceable for the UREs) through 10/28/09 (Mitigation Plan completion)**

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

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:
MITIGATION PLAN NO. **MIT-09-2538**
DATE SUBMITTED TO REGIONAL ENTITY **4/30/10**
DATE ACCEPTED BY REGIONAL ENTITY **5/21/10**
DATE APPROVED BY NERC **6/14/10**
DATE PROVIDED TO FERC **6/14/10**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE
N/A
MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **10/28/09**

DATE OF CERTIFICATION LETTER **4/30/10**[4]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **6/30/09**

DATE OF VERIFICATION LETTER **8/11/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **10/28/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
The UREs had already returned to full compliance at the time of the Spot Check. As noted above, the earlier version of the Cyber Incident response plan contained text adequately describing the procedure to characterize and classify events as reportable Cyber Security Incidents, as required by R1.1.

[4] The UREs' Certification of Mitigation Plan completion was included in the Mitigation Plan. The Settlement Agreement incorrectly states the Mitigation Plan completion date as June 30, 2009, the date determined by the UREs, instead of the date verified by Reliability*First*.

Additionally, a subsequent version of the Cyber Incident response plan included text adequately describing the plan must be updated within ninety (90) days of any changes, as required by R1.4.

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)
During the Spot Check, Reliability*First* reviewed the cyber security incident response plan.[5]

EXHIBITS:

SOURCE DOCUMENT
Reliability*First*'s Summary for Possible Violations of CIP-008-1 R1

MITIGATION PLAN AND CERTIFICATION BY REGISTERED ENTITY
UREs' Mitigation Plan MIT-09-2538 for CIP-008-1 R1 and Certification of Mitigation Plan Completion included therein submitted April 30, 2010

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan MIT-09-2538 Completion for CIP-008-1 R1 dated August 11, 2010

[5] CIP-008-2 R1.4 and CIP-008-3 R1.4, effective April 1, 2010 and October 1, 2010 respectively, have changed language from the original version of the Standard. The original ninety calendar days has been changed to thirty calendar days. On July 27, 2010, the UREs submitted cyber security incident response plan, which states that changes resulting from the lessons learned review must be implemented within 30 calendar days.