PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

August 31, 2011

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE**)** with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Documents attached thereto (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 URE have entered into a Settlement Agreement to resolve all outstanding issues arising from Reliability*First's* determination and findings of the violations of CIP-003-1 R (Requirement) 5, CIP-004-1 R2.1, CIP-004-1 R.3, CIP-002-1 R3.1, CIP-004-1 R4.2, CIP-006-1 R2, CIP-006-1 R1, and CIP-007-1 R6.3. According to the Settlement Agreement, URE stipulated to the facts in the Settlement Agreement and has agreed to the assessed penalty of seventy thousand dollars ($70,000), 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. With the exception of the violation of CIP-002-1, R3.1, which URE

[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

neither admits nor denies, URE admitted all the violation addressed in the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers: RFC201000648, RFC201000649, RFC201000650, RFC200900279, RFC201000280, RFC201000371, RFC201000379 and RFC201000615 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 May 5, 2011, by and between Reliability*First* and URE. The details of the findings and the basis for the penalty are set forth in the Disposition Documents. This NOP filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7, NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
NOC-879	RFC201000648	CIP-003-1	5	Lower	1/26/10-1/26/10	70,000
	RFC201000649	CIP-004-1	2.1	Medium[3]		
	RFC201000650	CIP-004-1	3	Medium[4]		
	RFC200900279	CIP-002-1	3.1	Lower[5]	7/01/09-6/1/11	
	RFC201000280	CIP-004-1	4.2	Medium[6]	1/25/10-2/4/10	
	RFC201000371	CIP-006-1	2	Medium	2/27/10-3/2/10	
	RFC201000379	CIP-006-1	1	Medium[7]	7/1/08-3/18/10	
	RFC201000615	CIP-007-1	6.3	Medium[8]	1/31/10 - 9/7/10	

[3] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 are each assigned a Lower Violation Risk Factor (VRF) and CIP-004-1 R2.1, R2.2 and R2.2.4 are each assigned a Medium VRF.
[4] CIP-004-1 R3 is assigned a Medium VRF and CIP-004-1 R3.1, R3.2 and R3.3 are each assigned a Lower VRF.
[5] CIP-002-1 R3 is assigned a High VRF and CIP-002-1 R3.1, R3.2 and R3.3 are each assigned a Lower VRF.
[6] CIP-004-1 R4 and R4.1 are each assigned a Lower VRF and CIP-004-1 R4.2 is assigned a Medium VRF.
[7] When NERC filed VRFs it originally assigned CIP-006-1 R1.5 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 February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-006-1 R1.5 was in effect from June 18, 2007 until February 2, 2009 when the Medium VRF became effective. CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 are each assigned a Medium VRF and CIP-006-1 R1.7, R1.8 and R1.9 are each assigned Lower VRF.
[8] CIP-007-1 R6, R6.4, and R6.5 are each assigned a Lower VRF and CIP-007-1 R6.1, R6.2 and R6.3 are each assigned a Medium VRF.

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

CIP-003-1 R5 (RFC201000648)

URE submitted a Self-Report to Reliability*First* identifying a violation of CIP-003-1 R5. Reliability*First* determined that URE improperly granted access to URE power plant to one contractor employee who was working on the development of cyber security controls on the plant's control system, in violation of this standard.

CIP-004-1 R2 (RFC201000649)

URE submitted a Self-Report to Reliability*First* identifying a violation of CIP-004-1 R2. Reliability*First* determined that as a result of granting the same contractor employee unauthorized access to its control system, URE failed to train the employee within 90 calendar days of granting such access, as required by the standard.

CIP-004-1 R3 (RFC201000650)

URE submitted a Self-Report to Reliability*First* identifying a violation of CIP-004-1 R3. Reliability*First* determined that as a result of granting the same contractor unauthorized access to its control system, URE failed to conduct a Personnel Risk Assessment on this individual within 30 days of being granted such unauthorized access, as required by the standard.

CIP-002-1 R3.1 (RFC200900279)
Reliability*First* conducted a CIP Spot Check of URE and determined that URE failed to identify as Critical Cyber Assets (CCAs) twelve remote workstations, which connect to URE's Energy Management System and allow for remote monitoring and control of the transmission system, in violation of this standard.

CIP-004-1 R4.2 (RFC201000280)
URE submitted a Self-Report to Reliability*First* for a violation of CIP-004-1 R4.2. Reliability*First* determined that URE failed to revoke the physical access of one subcontractor employee to its CCAs within seven days, in violation of the standard.

CIP-006-1 R2 (RFC201000371)
URE submitted a Self-Report to Reliability*First* for a violation of CIP-006-1 R2. Reliability*First* determined that URE failed to correctly implement its physical access controls by inadvertently leaving two doors offering direct access to URE's Physical Security Perimeter (PSP) unlocked for 56 and 83 hours, respectively, in violation of the standard.

CIP-006-1 R1 (RFC201000379)
URE submitted a Self-Report to Reliability*First* for a violation of CIP-006-1 R1. Reliability*First* determined that URE failed to identify an access point to a PSP by leaving an opening in a ceiling wall, which connected the PSP to a room outside the PSP, in violation of the standard.

CIP-007-1 R6.3 (RFC201000615)
URE submitted a Self-Report to Reliability*First* for a violation of CIP-007-1 R6.3. Reliability*First* determined that URE failed to file a Technical Feasibility Exception for some devices which could not log and report cyber security events because they were serially connected to one another and were unable to transmit information to devices to which they were not connected, in violation of the standard.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[9]

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,[10] 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 seventy thousand dollar ($70,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. the violations were not URE's first occurrence of violation of the subject NERC Reliability Standards;
2. URE self-reported seven out of the eight violations;
3. Reliability*First* considered an aggravating factor the fact that it discovered one of the violations at a Compliance Spot Check;
4. Reliability*First* reported that URE was cooperative throughout the compliance enforcement process;
5. Reliability*First* determined that the CIP compliance program at URE is operated at the parent company level and therefore all Self-Reports and violations should be investigated and reviewed at the enterprise level rather than within a single registered entity.
6. URE had a compliance program at the time of the violation and Reliability*First* considered the program to be a mitigating factor, as discussed in the Disposition Documents;
7. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

[9] *See* 18 C.F.R. § 39.7(d)(4).
[10] *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).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

8. 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
9. 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 seventy thousand dollars ($70,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Attachments to be included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between Reliability*First* and URE executed May 5, 2011, included as Attachment a:

i. URE's Self-Report for CIP-003-1 R5, included as Attachment A to the Settlement Agreement;

ii. URE's Mitigation Plan for CIP-003-1 R5, CIP-004-1 R2.1 and R3 (MIT-10-3257), included as Attachment B to the Settlement Agreement;

iii. URE's Certification of Mitigation Plan Completion for CIP-003-1 R5, CIP-004-1 R2.1 and R3 (MIT-10-3257), included as Attachment C to the Settlement Agreement;

iv. URE's Self-Report for CIP-004-1 R2.1, included as Attachment D to the Settlement Agreement;

v. URE's Self-Report for CIP-004-1 R3, included as Attachment E to the Settlement Agreement;

vi. Reliability*First's* Possible Violation Summery Sheet for CIP-002-1 R3.1, included as Attachment F to the Settlement Agreement;

vii. URE's Mitigation Plan for CIP-002-1 R3.1 (MIT-09-3508), included as Attachment G to the Settlement Agreement;

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

ix. URE's Mitigation Plan for CIP-004-1 R4.2 (MIT-10-2500), included as Attachment I to the Settlement Agreement;

x. URE's Certification of Mitigation Plan Completion for CIP-004-1 R4.2 (MIT-10-2500), included as Attachment J to the Settlement Agreement;

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

xi. Reliability*First's* Verification of Mitigation Plan Completion for CIP-004-1 R4.2 (MIT-10-2500), included as Attachment K to the Settlement Agreement;

xii. URE's Self-Report for CIP-006-1 R2, included as Attachment L to the Settlement Agreement;

xiii. URE's Mitigation Plan for CIP-006-1 R2 (MIT-10-2556), included as Attachment M to the Settlement Agreement;

xiv. URE's Certification of Mitigation Plan Completion for CIP-006-1 R2 (MIT-10-2556), included as Attachment N to the Settlement Agreement;

xv. Reliability*First's* Verification of Mitigation Plan Completion for CIP-006-1 R2 (MIT-10-2556), included as Attachment O to the Settlement Agreement;

xvi. URE's Self-Report for CIP-006-1 R1, included as Attachment P to the Settlement Agreement;

xvii. URE's Mitigation Plan for CIP-006-1 R1 (MIT-08-2550), included as Attachment Q to the Settlement Agreement;

xviii. URE's Certification of Mitigation Plan Completion for CIP-006-1 R1 (MIT-08-2550), included as Attachment R to the Settlement Agreement;

xix. Reliability*First's* Verification of Mitigation Plan Completion for CIP-006-1 R1 (MIT-08-2550), included as Attachment S to the Settlement Agreement;

xx. URE's Self-Report for CIP-007-1 R6.3, included as Attachment T to the Settlement Agreement; and

xxi. URE's Mitigation Plan for CIP-007-1 R6.3 1 (MIT-10-3044), included as Attachment U to the Settlement Agreement;

b) Reliability*First's* Verification of Mitigation Plan Completion for CIP-003-1 R5, CIP-004-1 R2.1 and R3 (MIT-10-3257) , included as Attachment b;

c) URE's Certification of Mitigation Plan Completion for CIP-002-1 R3.1 (MIT-09-3508), included as Attachment c;

d) Reliability*First's* Verification of Mitigation Plan Completion for CIP-002-1 R3.1 (MIT-09-3508), included as Attachment d;

e) URE's Certification of Mitigation Plan Completion for CIP-007-1 R6.3 1 (MIT-10-3044), included as Attachment e;

f) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 R6.3 1 (MIT-10-3044), included as Attachment f; and

g) Disposition Documents:

i. Disposition Document Common Information, included as Attachment g;

ii. Disposition Document for CIP -003-1 R5, CIP-004-1 R2 and CIP-004-1 R3, included as Attachment g-1;

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

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

iv. Disposition Document for CIP -004-1 R4.2, included as Attachment g-3;

v. Disposition Document for CIP -006-1 R2, included as Attachment g-4;

vi. Disposition Document for CIP -006-1 R1, included as Attachment g-5; and

vii. Disposition Document for CIP -007-1 R6.3, included as Attachment g-6.

A Form of Notice Suitable for Publication[11]

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

[11] *See* 18 C.F.R. § 39.7(d)(6).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Notices and Communications

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

Gerald W. Cauley* President and Chief Executive Officer David N. Cook* 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 gerry.cauley@nerc.net david.cook@nerc.net Michael D. Austin* Associate Attorney 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 mike.austin@rfirst.org Amanda E. Fried* Associate Attorney 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 amanda.fried@rfirst.org	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Davis Smith* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net davis.smith@nerc.net 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* Managing Enforcement Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 jason.blake@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

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

Respectfully submitted,

/s/ *Rebecca J. Michael*

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

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

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment g

Disposition Document Common Information

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment g

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS

Dated July 11, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity(URE)	**NCRXXXXX**	**NOC-879**

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	☒[2]
STIPULATES TO THE AGREEMENT		☒
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 **$70,000** FOR **EIGHT** VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

[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] URE neither admits nor denies the facts stipulated regarding the CIP-002-1 R3.1

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

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

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ NO ☐ UNDETERMINED ☐
EXPLAIN

Reliability*First* considered certain aspects of URE's compliance program as mitigating factors in determining the penalty amount.

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

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

YES ☐ NO ☒
IF YES, EXPLAIN

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

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☒ NO ☐
IF YES, EXPLAIN

Reliability*First* favorably considered that URE self-reported seven of the eight violations addressed in the Settlement Agreement. Furthermore, ReliabilityFirst favorably considered URE's cooperation at the Compliance Spot Check, throughout the subsequent enforcement process.

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☒ NO ☐
IF YES, EXPLAIN

Reliability*First* negatively considered that it discovered CIP-002-1 R3.1 at a Compliance Spot Check. Nevertheless, Reliability*First* favorably considered URE's cooperation at the Compliance Spot Check, throughout the subsequent enforcement process.

(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 REQUEST DATE
DATE: **2/7/11**OR N/A ☒

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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 -003-1 R5, CIP-004-1 R2 and CIP-004-1 R3

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

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000648	**RFC201000648**
RFC201000649	**RFC201000649**
RFC201000650	**RFC201000650**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-003-1[1]	**5**		**Lower**	**High**
CIP-004-1[2]	**2**	**1**	**Medium**[3]	**Lower**
CIP-004-1	**3**		**Medium**[4]	**Severe**

FACTS COMMON TO CIP-003-1 R5, CIP-004-1 R2.1 and R3

URE was working with an outside vendor to complete the development of cyber security controls on the control system for URE's facility.

The vendor identified which of its employees would be working on the control system, and URE required the vendor to administer and attest that it had completed the required training and performed background checks on those individuals, as required by CIP-004-1, R2 and R3, because the employees would have access to URE's Critical Cyber Assets (CCAs). The vendor provided a list of eight employees who had completed the required training and background checks.

In order to perform the required work on URE's system, URE required the vendor to use a Virtual Private Network (VPN) to access URE's system. By requiring use of a VPN, URE's personnel controlled access to its system within the Electronic Security Perimeter (ESP), and the vendor could not have initiated such access without the knowledge and authorization of URE's personnel. Furthermore, when URE's personnel grant access to its system within the ESP, the access expires automatically after 24 hours or after the user terminates access, whichever occurs first. A new access grant is required each time an individual needs access to the system.

[1] CIP-003-1 was in effect until March 31, 2010.
[2] CIP-004-1 was in effect until March 31, 2010.
[3] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 are each assigned a Lower Violation Risk Factor (VRF) and CIP-004-1 R2.1, R2.2 and R2.2.4 are each assigned a Medium VRF.
[4] CIP-004-1 R3 is assigned a Medium VRF and CIP-004-1 R3.1, R3.2 and R3.3 are each assigned a Lower VRF.

A URE Senior Engineer provided one of the vendor's technical support employees (Individual) with access to URE's system within the ESP in order to allow the Individual to troubleshoot a backup system and update anti-virus definitions on the system. The Individual was not on the vendor's list of eight authorized employees who had completed the requisite training and background checks. The Senior Engineer granted the Individual access through the firewall and created an account on the server within the ESP without first verifying that the Individual was on the approved list. As a result, the Individual accessed the system during the day of January 26, 2010.

Reliability*First* determined that the violations of CIP-003-1 R5, CIP-004-1 R2.1, and CIP-004- 1 R3 relate to this Individual's inappropriate access to URE's CCAs.

CIP-003-1 R5 (RFC201000648)

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

The purpose statement of CIP-003-1 provides in pertinent part: "Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-003-1 R5 provides in pertinent part:

> **R5. Access Control — The Responsible Entity[5] shall document and implement a program or managing access to protected Critical Cyber Asset information.**

VIOLATION DESCRIPTION

URE submitted a Self-Report to Reliability*First* identifying a violation of CIP-003-1 R5. URE specified that it improperly granted access to the Individual, who did not have the training or background checks required by URE's documented access control program.

Therefore, Reliability*First* determined that URE violated CIP-003-1 R5 by failing to fully implement its documented access control program for managing access to its protected CCAs.

[5] Within the text of Standard CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

CIP-004-1 R2.1 (RFC201000649)

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 in pertinent part:

R2. Training — The Responsible Entity 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.

> **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

URE submitted a Self-Report to Reliability*First* identifying a violation of CIP-004-1 R2 and specifying that as a result of granting the Individual unauthorized access to its CCAs, it failed to train the Individual within 90 calendar days of granting such access, as required by the standard.

Reliability*First* determined that URE violated CIP-004-1 R2.1 for failure to ensure that all personnel having authorized cyber access to CCAs were trained within 90 calendar days of gaining such access.

CIP-004-1 R3 (RFC201000650)

CIP-004-1 R3 provides in pertinent part:

> **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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access.**

VIOLATION DESCRIPTION

URE submitted a Self-Report, identifying a violation of CIP-004-1 R3. URE stated that it failed to conduct a Personnel Risk Assessment (PRA) on the Individual pursuant to its documented PRA program. URE failed to ensure that the Individual had a completed PRA within 30 days of being granted cyber access to URE's system, as required by the standard.

Therefore, Reliability*First* determined that URE violated CIP-004-1 R3 by failing to conduct a PRA for personnel with authorized cyber access to URE's system within 30 days of granting such access.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL:
RFC201000648, RFC201000649, RFC201000650

Reliability*First* determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because URE granted access to protected CCAs to only one individual. Also, the Individual could not access the account after January 26, 2010 (the day the access occurred) due to URE's electronic security that automatically cancels access within 24 hours.

The Individual could not have gained access to the VPN after January 26, 2010 without the knowledge and authorization of URE's personnel. Moreover, prior to the CIP Standards becoming mandatory, URE had granted the Individual access to its system because the Individual assisted in designing the system, and as a result, URE was familiar with the Individual in question.

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)

RFC201000648, RFC201000649, RFC201000650: 1/26/10 (when URE granted unauthorized access to the Individual) through 1/26/10 (access to the Individual's account automatically expired)

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

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.
RFC201000648, RFC201000649, RFC201000649 **MIT-10-3257**

DATE SUBMITTED TO REGIONAL ENTITY **12/10/10**
DATE ACCEPTED BY REGIONAL ENTITY **1/10/11**
DATE APPROVED BY NERC **1/31/11**
DATE PROVIDED TO FERC **2/3/11**

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 **4/21/10**

DATE OF CERTIFICATION LETTER **3/3/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **4/21/10**

DATE OF VERIFICATION LETTER **5/9/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **4/21/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

After discovering that the Individual was granted unauthorized access, URE disabled the Individual's account and removed it from the control system within the ESP. URE notified the vendor's Technical Support about the event and discussed with the vendor the requirement to have only trained and screened personnel request access to this particular system.

Also, URE implemented a process for approval and tracking of trained and screened personnel with access to the CCA via an electronic ticketing system.

Under the new centralized process, access to CCA resources, both physical and electronic, is requested through a procedure, which includes the use of electronic request form. Only the manager of the person needing access, including a manager of a contractor, is allowed to request access to CCA resources. Forms generated by anyone other than the manager are rejected. The electronic form also is tied to URE's management and tracking system. The electronic form provides tracking of changes and access requests to resources within the CCA spaces. All other requests are handled through URE's corporate change management and access request processes.

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 ticket request example report. 0.**
- **Request ticket screenshots.**
- **NERC access services portal.**
- **User access request-electronic and physical.**
- **A screenshot that shows the specific user in question had the account disabled on the machine the specific user was given inappropriate access.**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-003-1 R5
URE's Self-Report for CIP-004-1 R2.1
URE's Self-Report for CIP-004-1 R3

MITIGATION PLAN
URE's Mitigation Plan MIT-10-3257 for CIP-003-1 R5, CIP-004-1 R2.1 and CIP-004-1 R3

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion (MIT-10-3257)

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion (MIT-10-3257)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP -002-1 R3.1

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment g-2

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC200900279	**RFC200900279**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-002-1	**3**	**1**	**Lower**[1]	**Severe**

CIP-002-1 R3.1 (RFC200900279)

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:

> **"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 R3.1 provides in pertinent part:

> **R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity 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.**

[1] CIP-002-1 R3 is assigned a High VRF and CIP-002-1 R3.1, R3.2 and R3.3 are each assigned a Lower VRF.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

VIOLATION DESCRIPTION

Reliability*First* conducted a CIP Spot Check of URE.

Reliability*First* determined that URE operates servers, which are identified as Critical Cyber Assets (CCAs) because they enable remote access to URE's Energy Management System (EMS). URE had identified 39 workstations with access to the servers as CCAs, but failed to identify 12 remote workstations, which are permitted to use the servers, as CCAs.

Reliability*First* determined that these remote workstations are essential to the reliable operation of the CCAs and URE's backup control center because it is possible for a user to connect to the EMS from these workstations to monitor and control the transmission system. Reliability*First* determined that URE incorrectly considered these workstations to be non-essential to the operation of the CCAs. Since the workstations use a routable protocol to communicate outside the Electronic Security Perimeter (ESP), they are essential to the operation of the CCAs.

Reliability*First* determined that URE violated CIP-002-1 R3.1 for failure to identify the 12 remote workstations as CCAs.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that this violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because URE blocks outside access to its EMS application. In addition, the authentication process for accessing the EMS from these workstations requires three or more levels of authentication, and each level is administered by a separate group within URE. As a result, an individual must be purposely granted access through the connection to access the EMS.[2] Further, the 12 workstations have been located within URE's Physical Security Perimeter (PSP) at all relevant times.

URE has established additional controls, such as a prohibition on copy and paste, local printing, and remote drive and device mapping on the trusted systems' servers. URE only allows users to print important information using the printers located in secure spaces.

[2] In order to access URE's trusted system, which enables access to the EMS application, the system requires several controls at the various access points to ensure the user's authenticity. For example, remote access to URE's trusted system requires a dedicated account in the trusted system such that anonymous logins are prohibited. All users of these workstations have been CIP screened and trained. Furthermore, the server reports user access information including the user's identity, the time of log in, and the applications accessed.

Reliability*First* determined that all of the above mentioned controls illustrate that information on URE's system remains local to the servers and cannot be removed despite being accessed from the remote workstations.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATES: **7/01/09 through 06/1/11 (Mitigation Plan completion).**

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

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-3508**
DATE SUBMITTED TO REGIONAL ENTITY	**3/10/11**
DATE ACCEPTED BY REGIONAL ENTITY	**3/28/11**
DATE APPROVED BY NERC	**4/21/11**
DATE PROVIDED TO FERC	**4/21/11**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**6/1/11**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**6/1/11**[3]
DATE OF CERTIFICATION LETTER	**6/2/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**6/1/11**
DATE OF VERIFICATION LETTER	**8/9/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**6/1/11**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE took the following actions to mitigate the violation:

1. **Removed remote access to the EMS control function from the remote workstations that are not defined as CCAs.**

2. **Established PSPs and ESPs for all locations where monitoring and control functions of the EMS are allowed.**

3. **Identified the remote workstations as CCAs.**

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)

- **Removal of remote access to EMS control functions from non-CCAs consists of three parts:**
  - **Evidence that shows the revised configuration to permit only a very restricted set of clients to access the server session that permits control of bulk electric system functions.**
  - **Evidence that shows that permissions for control access must be granted to both the user and the workstation from which access is initiated.**
  - **Evidence that shows this change being communicated to URE's users.**
  - **Evidence that shows restriction of access on the workstation level via firewall rule.**
  - **Evidence that shows a test of unauthorized access resulting in an error message.**

[3] The Certification of Mitigation Plan Completion was signed on June 3, 2011.

- **Establishment of a PSP and ESP for all locations where monitoring and control function of the EMS is allowed.**
  - **Evidence that states that no PSP was added as a result of this mitigation. Rather, URE limited workstation privileges so that no workstation outside of a PSP can perform control functions on the bulk electric system.**
  - **Evidence that shows the modification of the ESPs via firewall rule change tickets to implement the new configuration.**
- **Identification of the appropriate workstations as CCAs.**
  - **Evidence that shows change ticket summaries for operator workstations at URE's backup locations, implementing the necessary configuration for control of the bulk electric system in emergency situations.**
  - **Evidence that shows the final implementation change tickets for firewall rules and operator consoles.**

EXHIBITS:

SOURCE DOCUMENT
ReliabilityFirst's Possible Violation Summary Sheet for CIP-002-1 R3.1

MITIGATION PLAN

URE's Mitigation Plan MIT-09-3508 for CIP-002-1 R3.1

CERTIFICATION BY REGISTERED ENTITY

URE's Certification of Mitigation Plan Completion (MIT-09-3508)

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion (MIT-09-3508)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP -004-1 R4.2

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

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000280	**RFC201000280**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**4**	**2**	**Medium**[1]	**Moderate**

CIP-004-1 R4.2 (RFC201000280)

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 R4.2 provides in pertinent part:

> **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.**
>
> > **R4.2. 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

URE submitted a Self-Report to Reliability*First* for a violation of CIP-004-1 R4.2. URE stated that it employed a contractor firm (Company) to manage certain projects within URE, and that several subcontractors of the Company had physical

[1] CIP-004-1 R4 and R4.1 are each assigned a Lower VRF and CIP-004-1 R4.2 is assigned a Medium VRF.
[2] Within the text of Standard CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

access to URE's system control center, which includes Critical Cyber Assets (CCAs).

On January 18, 2010, one subcontractor firm informed the Company that one of the subcontractor's employees (Employee) no longer required physical access to URE's facility. The Company did not submit a request with URE to revoke the Employee's access. URE subsequently discovered that this Employee had access to the facility and revoked the access on February 4, 2010.

Reliability*First* determined that URE violated CIP-004-1 R4.2 for failure to revoke the Employee's physical access to CCAs within seven days, as required by the standard.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because URE ensured that the Employee was trained and screened prior to receiving access. The Employee neither accessed nor attempted to access the URE facility after the work was completed.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATES: **1/25/10 (seven calendar days after the Employee no longer required access) through 2/4/10 (date URE revoked the Employee's access).**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **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	☒

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2500**
DATE SUBMITTED TO REGIONAL ENTITY	**5/6/10**[3]
DATE ACCEPTED BY REGIONAL ENTITY	**5/7/10**
DATE APPROVED BY NERC	**5/26/10**
DATE PROVIDED TO FERC	**5/26/10**

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**4/1/10**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**4/1/10**
DATE OF CERTIFICATION LETTER	**6/8/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**4/1/10**
DATE OF VERIFICATION LETTER	**6/29/10**[4]
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**4/1/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE implemented the following two new procedural changes associated with its CCAs access control management:

1. A centralized form for requesting and granting access to all CCAs resources was developed and implemented.

2. Temporary physical access is no longer allowed. Physical access is granted on a "permanent" basis, while individuals needing short-term access are escorted.

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)

1. An email requesting changes on behalf of the URE's CIP Team.
2. flowchart for the access request process.
3. location where users can access the NERC access request tool.

[3] The Mitigation Plan was signed on April 15, 2010.
[4] The Verification of Mitigation Plan Completion letter states that URE submitted its Mitigation Plan on April 15, 2010.

4. Screenshot that shows the new request form and the Corporate form.
5. A list of access requests and their various status states.
6. Report of the Facilities access review

EXHIBITS:

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

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2500 for CIP-004-1 R4.2

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion (MIT-10-2500)

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion (MIT-10-2500)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP -006-1 R2

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

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000371	**RFC201000371**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-006-1	**2**		**Medium**[1]	**High**

CIP-006-1 R2 (RFC201000371)

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

CIP-006-1 R2 provides in pertinent part:

> **R2. Physical Access Controls — The Responsible Entity[2] shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week.**

VIOLATION DESCRIPTION

URE submitted a Self-Report to Reliability*First* for non-compliance with CIP-006-1 R2. In the Self-Report, URE stated that during a training exercise conducted at the security console located at a URE office, a security officer inadvertently unlocked a door that serves as an access point to URE's Physical Security Perimeter (PSP) to a support operations center. URE discovered that the door was unlocked and had been unlocked for 56 hours before discovery.

[1] When NERC filed VRFs it originally assigned CIP-006-1 R1.5 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 February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-006-1 R1.5 was in effect from June 18, 2007 until February 2, 2009 when the Medium VRF became effective. CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 are each assigned a Medium VRF and CIP-006-1 R1.7, R1.8 and R1.9 are each assigned Lower VRF.

[2] Within the text of Standard CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

Subsequently, URE performed a comprehensive review of the status of all doors providing access points to URE's PSPs. URE discovered that the same security officer had inadvertently unlocked an additional door at one of their plants, during the training exercise. This door remained unlocked for approximately 83 hours. In both instances, the security officer believed that the system was operating in a training mode. Thus, URE failed to manage physical access to two access points to a PSP.

Reliability*First* determined that URE violated CIP-006-1, R2 for failure to correctly implement physical access controls at access points to its PSPs.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because in order to gain access to the unlocked doors, an individual would have to gain access through the fence surrounding the complex, through the door to the building, and through another interior door. An individual must have varying levels of badge access to gain access through each of these access points. Also, security staff monitors both locations 24 hours a day, seven days a week.

Therefore, Reliability*First* determined that it was unlikely that an unauthorized user could proceed through all access points and gain unauthorized access to URE's system.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATES: **2/27/10 (date the doors were unlocked) through 3/2/10 (date URE locked both doors)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **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 VIOLATIONS	YES	☐	NO	☒

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2556**
DATE SUBMITTED TO REGIONAL ENTITY	**5/12/10**
DATE ACCEPTED BY REGIONAL ENTITY	**6/4/10**[3]
DATE APPROVED BY NERC	**6/15/10**
DATE PROVIDED TO FERC	**6/28/10**

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**4/8/10**
DATE OF CERTIFICATION LETTER	**6/15/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**4/8/10**
DATE OF VERIFICATION LETTER	**7/14/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**4/8/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

1. **URE revised its security console procedures to prohibit operator training when the actual production system application is operating and to require a review of the lock and unlock status of all access points to its PSPs.**

2. **URE retrained its security console operators on the relevant standards and modified its security console application to allow only managers to remotely unlock access points to the PSPs, thus preventing security console operators from remotely unlocking access points.**

3. **URE restricted user privileges permitting the locking and unlocking of access points to PSPs to supervisory personnel.**

[3] The Verification of Mitigation Plan completion has a typographical error that states Reliability*First* accepted the Mitigation Plan on May 20, 2010.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

1. **Revised security console procedures;**
2. **Memo Documenting Training;**
3. **Screen Shot of Training Records;**
4. **Sample Test for NERC training;**
5. **Response procedures;**
6. **Application for programming change;**
7. **Modified security console application; and**
8. **List of security supervisors.**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-006-1 R2

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2556 for CIP-006-1 R2

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion (MIT-10-2556)

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion (MIT-10-2556)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP -006-1 R1

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment g-5

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000379	**RFC201000379**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-006-1	**1**		**Medium**[1]	**Moderate**

CIP-006-1 R1 (RFC201000379)

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

CIP-006-1 R1 provides in pertinent part:

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

VIOLATION DESCRIPTION

URE submitted a Self-Report to Reliability*First* for a violation of CIP-006-1 R1. URE stated that it failed to control entry at an access point to one of its Physical Security Perimeters (PSPs). While performing a review of the PSP at a facility,

[1] When NERC filed VRFs it originally assigned CIP-006-1 R1.5 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 February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-006-1 R1.5 was in effect from June 18, 2007 until February 2, 2009 when the Medium VRF became effective. CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 are each assigned a Medium VRF and CIP-006-1 R1.7, R1.8 and R1.9 are each assigned Lower VRF.

[2] Within the text of Standard CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

which includes a control center, URE discovered a 15 inch by 20 inch ceiling opening in a wall between the PSP and a restroom outside the PSP.

The wall opening remained from the original Heating, Ventilation and Air Conditioning design of the building and was located within a remote non-public space and above the drop ceiling of the Energy Management System (EMS) equipment room. The opening was covered with a sheet of plastic and was secured with duct tape. URE had not previously known about this opening and therefore did not repair it.

Reliability*First* determined that URE violated CIP-006-1 R1 for failure to identify an access point to the PSP and for failing to take measures to control entry at that access point.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because there was an additional physical security barrier at the site. Security staff monitors the location 24 hours a day, and URE's operations personnel are also present 24 hours a day. In addition, the opening in question was less accessible because it was located above a false ceiling, and was not visible as a potential entry point because of the plastic sheeting on the ceiling.

Therefore, Reliability*First* determined that it was highly unlikely that an unauthorized user would enter the site and gain access to the control center. Moreover, URE found no evidence suggesting that anyone entered the site through this opening.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATES: **7/1/09 (date URE was required to comply with CIP-006-1 R1) through 3/18/10 (URE sealed the opening)**

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-08-2550**
DATE SUBMITTED TO REGIONAL ENTITY	**5/28/10**
DATE ACCEPTED BY REGIONAL ENTITY	**6/11/10**
DATE APPROVED BY NERC	**6/25/10**
DATE PROVIDED TO FERC	**6/28/10**

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**3/18/10**
DATE OF CERTIFICATION LETTER	**6/15/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**3/18/10**
DATE OF VERIFICATION LETTER	**7/13/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**3/18/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE permanently sealed the opening on the same day it was discovered.

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)

Six photos - two photos before repairs, and four photos showing various stages of repair.

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-006-1 R1

MITIGATION PLAN
URE's Mitigation Plan MIT-08-2550 for CIP-006-1 R1

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion (MIT-08-2550)

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion (MIT-08-2550)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP -007-1 R6.3

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment g-6

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000615	**RFC201000615**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	**6**	**3**	**Medium**[1]	**Severe**

CIP-007-1 R6.3 (RFC201000615)

The purpose statement of CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities 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."

CIP-007-1 R6.3 provides in pertinent part:

> **R6. Security Status Monitoring — The Responsible Entity[2] 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.**
>
> > **R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP- 008.**

VIOLATION DESCRIPTION

URE submitted a Self-Report to Reliability*First* for non-compliance with CIP-007-1 R6.3. URE stated that it had discovered that some devices at multiple substations could not log and report cyber security events because the devices were serially

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

[2] Within the text of Standard CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

connected to one another and were unable to transmit information to devices to which they were not connected. In addition, URE's infrastructure did not support retrieving the limited security status information that the devices could provide.

To effectuate compliance with this standard, URE could have filed a Technical Feasibility Exception (TFE) request with Reliability*First* in accordance with Appendix 4D of the NERC Rules of Procedure, but URE failed to do so.

Therefore, Reliability*First* concluded that URE violated CIP-007-1 R6.3 for failure to maintain logs of system events related to cyber security.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violation did not pose a serious or substantial risk to the bulk power system (BPS) because although some of the devices that lacked the capability to maintain logs of system events were located within a blackstart facility, all were serially connected within each facility, had no remote capability, and were located within a Physical Security Perimeter. Because devices connected in a series in general do not affect one another in the event of an outage, serial connections reduce the likelihood of the failure of multiple devices in the event of a cyber incident.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATES: **1/31/10 (date URE was required to comply with the TFE requirements of CIP-007-1 R6.3) through 9/7/10 (date URE submitted a TFE to Reliability*First*)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **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

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-3044**
DATE SUBMITTED TO REGIONAL ENTITY	**9/10/10**
DATE ACCEPTED BY REGIONAL ENTITY	**11/11/10**
DATE APPROVED BY NERC	**11/23/10**
DATE PROVIDED TO FERC	**11/23/10**

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**9/7/10**
DATE OF CERTIFICATION LETTER	**3/3/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**9/7/10**
DATE OF VERIFICATION LETTER	**3/24/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**9/7/10**[3]

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE submitted a TFE for CIP-007-1 R6.3, which identified the number of devices, types of devices, and a summary of mitigating actions for the devices that did not meet strict compliance with the standard.

URE submitted evidence obtained from the vendors in support of its claim that the devices were unable to perform logging and event reporting.

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's TFE documentation

[3] Reliability*First* performed a separate Mitigation Plan verification and found that URE completed the Mitigation Plan by virtue of submitting a TFE request.

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R6.3

MITIGATION PLAN
URE's Mitigation Plan MIT-10-3044 for CIP-007-1 R6.3

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion (MIT-10-3044)

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion (MIT-10-3044)