PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 28, 2011

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Documents (Attachment f), 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-005-1 Requirement (R) 2.4, CIP-006-1 R1.1, and CIP-007-1 R5.2.1 and R5.2.3. According to the Settlement Agreement, URE neither admits nor denies the violations, and has agreed to the assessed penalty of eighteen thousand dollars ($18,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers RFC201000273, RFC201000274, RFC201000277

[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

and RFC201000278 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 March 9, 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-837	RFC201000273	CIP-005-1	2.4	Medium[3]	1/1/10 – 1/29/10	18,000
	RFC201000274	CIP-006-1	1.1	Medium[4]	1/1/10 – 1/28/10	
	RFC201000277	CIP-007-1	5.2.1	Medium[5]	1/1/10 – 11/1/10	
	RFC201000278	CIP-007-1	5.2.3	Medium[6]	1/1/10 – 6/30/10	

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

CIP-005-1 R2.4 - OVERVIEW

As a result of a Self-Report submitted by URE, Reliability*First* determined that URE did not implement any procedural or technical controls at the access point to ensure the authenticity of users accessing the Electronic Security Perimeter (ESP), as required by the standard.

CIP-006-1 R1.1 - OVERVIEW

As a result of a Self-Report submitted by URE, Reliability*First* determined that URE failed to ensure that certain Critical Cyber Assets resided within an identified Physical Security Perimeter.

CIP-007-1 R5.2.1 - OVERVIEW

As a result of a Self-Report submitted by URE, Reliability*First* determined that URE did not minimize and manage the scope and acceptable use of generic accounts for a total of nine servers

[3] CIP-005-1 R2, R2.1, R2.2, R2.3, and R2.4 are each assigned a Medium Violation Risk Factor (VRF) and CIP-005-1 R2.5, R2.5.1, R2.5.2, R2.5.3, R2.5.4, and R2.6 are each assigned a Lower VRF.
[4] 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 a Lower VRF.
[5] CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, and R5.2.2 are each assigned a Lower VRF and CIP-007-1 R5.1, R5.1.3, R5.2.1 and R5.2.3 are each assigned a Medium VRF.
[6] *Id.*

and operations workstations, as required by the standard, by the removal, disabling, or renaming of such accounts where possible.

CIP-007-1 R5.2.3 - OVERVIEW

As a result of a Self-Report submitted by URE, Reliability*First* determined that URE did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges, as required by the standard.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[7]

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,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on June 10, 2011. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of an eighteen thousand dollar ($18,000) 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 constituted URE's first occurrence of violation of the subject NERC Reliability Standards;
2. URE self-reported the violations;
3. Reliability*First* reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which Reliability*First* considered a mitigating factor, as discussed in the Common Disposition Document;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. Reliability*First* determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), as discussed in the Disposition Documents; and
7. Reliability*First* reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[7] *See* 18 C.F.R. § 39.7(d)(4).

[8] *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).

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of eighteen thousand dollars ($18,000) 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 March 9, 2011, included as Attachment a;

   i. URE's Mitigation Plan MIT-10-2453 for CIP-005-1 R2.4, included as Attachment A to the Settlement Agreement;

   ii. URE's Certification of Mitigation Plan Completion for CIP-005-1 R2.4, included as Attachment B to the Settlement Agreement;

   iii. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-005-1 R2.4, included as Attachment C to the Settlement Agreement;

   iv. URE's Mitigation Plan MIT-10-2454 for CIP-006-1 R1.1, included as Attachment D to the Settlement Agreement;

   v. URE's Certification of Mitigation Plan Completion for CIP-006-1 R1.1, included as Attachment E to the Settlement Agreement;

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

   vii. URE's Mitigation Plan MIT-10-2400 for CIP-007-1 R5.2.1, included as Attachment G to the Settlement Agreement;

   viii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R5.2.1, included as Attachment H to the Settlement Agreement;

   ix. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 R5.2.1 , included as Attachment I to the Settlement Agreement;

   x. URE's Mitigation Plan MIT-10-2401 for CIP-007-1 R5.2.3, included as Attachment J to the Settlement Agreement;

   xi. URE's Certification of Mitigation Plan Completion for CIP-007-1 R5.2.3, included as Attachment K to the Settlement Agreement; and

   xii. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 R5.2.3, included as Attachment L to the Settlement Agreement.

b) URE's Self-Report for CIP-005-1 R2.4, included as Attachment b;

c) URE's Self-Report for CIP-006-1 R1.1, included as Attachment c;

d) URE's Self-Report for CIP-007-1 R5.2.1, included as Attachment d;

e) URE's Self-Report for CIP-007-1 R5.2.3, included as Attachment e; and

f) Common Disposition Document, included as Attachment f;

   i. Disposition Document for CIP-005-1 R2.4, included as Attachment f-1;

   ii. Disposition Document for CIP-006-1 R1.1, included as Attachment f-2; and

   iii. Disposition Document for CIP-007-1 R5.2.1 and R5.2.3, included as Attachment f-3.

A Form of Notice Suitable for Publication[9]

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

[9] *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	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
David J. Rosenfeldt* Associate Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 david.rosenfeldt@rfirst.org	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
*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.	L. Jason Blake* Corporate Counsel Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 jason.blake@rfirst.org
	Megan E. Gambrel* Associate Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 megan.gambrel@rfirst.org

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 f

Common Disposition Document

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

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS
Dated June 10, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-837**

REGIONAL ENTITY
Reliability*First* Corporation (Reliability*First*)

IS THERE A SETTLEMENT AGREEMENT YES ☒ NO ☐

WITH RESPECT TO THE VIOLATION(S), REGISTERED ENTITY

NEITHER ADMITS NOR DENIES IT (SETTLEMENT ONLY) YES ☒
ADMITS TO IT YES ☐
DOES NOT CONTEST IT (INCLUDING WITHIN 30 DAYS) YES ☐

WITH RESPECT TO THE ASSESSED PENALTY OR SANCTION, REGISTERED ENTITY

ACCEPTS IT/ DOES NOT CONTEST IT YES ☒

I. PENALTY INFORMATION

TOTAL ASSESSED PENALTY OR SANCTION OF **$18,000** FOR **FOUR** 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.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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
At the time of the violations, URE had in place an internal compliance program (ICP) that was reviewed by Reliability*First* and Reliability*First* considered certain aspects of URE's ICP as mitigating factors.

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

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

YES ☐ NO ☒
IF YES, EXPLAIN

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

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

SETTLEMENT REQUEST DATE
DATE: **1/17/11** OR N/A ☐
NOTICE OF CONFIRMED VIOLATION ISSUED
DATE: OR N/A ☒

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

REGISTERED ENTITY RESPONSE CONTESTED
FINDINGS ☐ PENALTY ☐ BOTH ☐ DID NOT CONTEST ☒
HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-005-1 R2.4

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

DISPOSITION OF VIOLATION
Dated June 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000273	**RFC201000273**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-005-1	**2**	**2.4**	**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-005-1 provides, in pertinent part: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-005-1 R2.4 provides:

> **R2. Electronic Access Controls — The Responsible Entity[3] shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).**
>
> **R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.**

(Footnote added).

---

[1] CIP-005-1 R2, R2.1, R2.2, R2.3,and R2.4 are each assigned a Medium Violation Risk Factor (VRF) and CIP-005-1 R2.5, R2.5.1, R2.5.2, R2.5.3, R2.5.4, and R2.6 are each assigned a Lower VRF.

[2] At the time of the violations, no VSLs were in effect for CIP-005. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[3] Within the text of Standard CIP-005, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

VIOLATION DESCRIPTION

URE submitted a Self-Report to Reliability*First* concerning a violation of CIP-005-1 R2.4 due to URE's failure to implement any procedural or technical controls at the access point to ensure the authenticity of users accessing the Electronic Security Perimeter (ESP).

URE discovered the violation during a firewall rule-set review. URE found that it was unable to identify and authenticate unique users accessing URE's ESP. Specifically, URE determined that a user outside the ESP possibly could use a remote desktop protocol and generic account to connect to a Critical Cyber Asset (CCA) within the ESP without first uniquely identifying oneself.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because only eight URE employees had access to the generating unit within the ESP, and those eight employees were authorized and had completed CIP training and personnel risk assessment (PRA) requirements. Moreover, the CCAs at issue in this violation are part of URE's unit generation control system, which is one of URE's smallest generators. URE's power flow studies show that the loss of the generating unit would have a minimal impact on URE's operations.

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) **1/1/10 through 1/29/10 (Mitigation Plan completion)**

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 ☒

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2453**
DATE SUBMITTED TO REGIONAL ENTITY	**4/1/10**
DATE ACCEPTED BY REGIONAL ENTITY	**4/15/10**
DATE APPROVED BY NERC	**4/30/10**
DATE PROVIDED TO FERC	**5/3/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**1/29/10**
DATE OF CERTIFICATION LETTER	**4/1/10**[4]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**1/29/10**
DATE OF VERIFICATION LETTER	**4/19/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**1/29/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

- **URE restricted unauthenticated remote desktop protocol access to the ESP. This action was completed on January 26, 2010.**
- **URE implemented a change request providing alternate access to the ESP. Access now requires operator authentication and eliminates the need for the firewall rule. This action was completed on January 29, 2010.**

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

- **Firewall change activity report**
- **Change request for firewall rules**
- **Before and after configuration diagrams**

[4] The Certification of Completion is dated March 19, 2010 and signed on April 1, 2010.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2453
CERTIFICATION BY REGISTERED ENTITY

URE's Certification of Mitigation Plan Completion

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-006-1 R1.1

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

DISPOSITION OF VIOLATION
Dated June 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000274	**RFC201000274**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-006-1	**1**	**1.1**	**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-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 R1.1 provides:

> **R1. Physical Security Plan — The Responsible Entity[3] shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:**
>
> **R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets**.

(Footnote added).

[1] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 are each assigned a Medium Violation Risk Factor (VRF) and CIP-006-1 R1.7, R1.8 and R1.9 are each assigned a Lower VRF.
[2] At the time of the violations, no VSLs were in effect for CIP-006. 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-006, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

VIOLATION DESCRIPTION

URE submitted a Self-Report to Reliability*First* concerning a violation of CIP-006-1 R1.1 due to URE's failure to secure Critical Cyber Assets (CCAs) within an identified Physical Security Perimeter (PSP).

During a vendor site visit, URE discovered that the control processors for a generation station unit were running a routable protocol and were in fact CCAs. After determining that the control processors were CCAs, URE determined it was in violation of the standard because the control processors for the generating plant did not reside within an identified PSP. URE determined that these control processors were not classified as CCAs because information provided by the vendor indicated that the control processors were not using a routable protocol.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because only URE personnel with an authorized key card access device had access to both the generation plant and to the control processors contained within. In addition, the only generating unit with which the control processors are associated is one of URE's smallest generators. URE's power flow studies show that the loss of this generating unit would have a minimal impact on URE's operations.

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) **1/1/10 through 1/28/10 (Mitigation Plan completion)**

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

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

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2454**
DATE SUBMITTED TO REGIONAL ENTITY	**3/19/10**
DATE ACCEPTED BY REGIONAL ENTITY	**4/15/10**
DATE APPROVED BY NERC	**4/30/10**
DATE PROVIDED TO FERC	**5/3/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**1/28/10**
DATE OF CERTIFICATION LETTER	**3/19/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**1/28/10**
DATE OF VERIFICATION LETTER	**4/19/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**1/28/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

- **URE solicited and received a quote from URE's Security vendor, to create PSPs for two plant locations at the generating station. This action was completed on January 7, 2010**
- **URE approved the quote to create PSPs at the generating station. This action was completed on January 8, 2010.**
- **URE accepted a quote from an electrical contractor, to install all data, video, and power cabling for URE's facilities. This action was completed on January 13, 2010.**
- **The two vendors finished installation and testing of equipment. This action was completed on January 27, 2010**

- **URE's PSPs were in place and fully functional. This action was completed on January 28, 2010.**

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

- **Evidence that shows equipment installed for creation of PSPs at the generating station from URE's security vendor and an electrical contractor.**

- **Evidence that shows implementation of proper controls in new PSPs.**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report dated January 29, 2010

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2454

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007-1 R5.2.1 and R5.2.3

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

DISPOSITION OF VIOLATION
Dated June 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000277	**RFC201000277**
RFC201000278	**RFC201000278**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)[1]
CIP-007-1	**5**	**5.2.1**	**Medium[2]**	**N/A**
CIP-007-1	**5**	**5.2.3**	**Medium[3]**	**N/A**

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

The purpose statement of CIP-007-1 provides: "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 R5 provides, in pertinent part:

> **R5. Account Management — The Responsible Entity[4] shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.**
>
> **R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.**

---

[1] At the time of the violations, no VSLs were in effect for CIP-007. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[2] CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, and R5.2.2 are each assigned a Lower VRF and CIP-007-1 R5.1, R5.1.3, R5.2.1 and R5.2.3 are each assigned a Medium VRF.

[3] *Id.*

[4] Within the text of Standard CIP-007, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

VIOLATION DESCRIPTION

RFC201000277

URE submitted a Self-Report to Reliability*First* concerning a violation of CIP-007-1 R5.2.1 due to URE's failure to minimize and manage the scope and acceptable use of generic accounts.

Reliability*First* determined that URE's non-compliance with the standard resulted from nine total servers and operator workstations with default accounts that could not be renamed, removed, or disabled in accordance with CIP-007-1 R5.2.1 due to system architecture supplied by the vendor. Moreover, URE could not change the passwords to the servers and operator workstations in question in accordance with the standard due to the system architecture. To mitigate the alleged violation, URE acquired the necessary system architecture from its vendor to achieve compliance which provided for default account renaming, removal, disabling and password changes.

RFC201000278

URE submitted a Self-Report to Reliability*First* concerning a violation of CIP-007-1 R5.2.3 due to URE's failure to implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges.

URE discovered that one of its applications, that controls user authentication and provides user activity logging, was malfunctioning due to a corruption in its database that originated from the vendor. When a user account expired, the user was prompted to change his or her password and was able to change that password. Nevertheless, after the password change occurred, the application erroneously recognized the user account as expired and denied the user access to the account. In order to work around the database corruption issue and to prevent being locked out of their accounts, URE system operators remained logged into the application on a

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

long-term basis.[5] This long-term access constitutes a failure to implement a policy to minimize and manage the scope and acceptable use of accounts.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because access to the operating servers and operator workstations was limited to personnel, including system operators, who received authorization for access, completed cyber security training, and had an acceptable personnel risk assessment. Moreover, the Critical Cyber Asset at issue in this alleged violation is part of URE's unit generation control system. This generating unit is one of URE's smallest generators. URE's power flow studies show that the loss of the generating unit would have a minimal impact on URE's operations.

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)

RFC201000277: 1/1/10 through 11/1/10 (Mitigation Plan completion)

RFC201000278: 1/1/10 through 6/30/10 (Mitigation Plan completion)

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	☒

[5] To ensure operational consistency and prevent the next operator from being unable to log in and control the Critical Cyber Asset, the system operator had to avoid logging out of the system.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **RFC201000277: MIT-10-2400**
RFC201000278: MIT-10-2401

DATE SUBMITTED TO REGIONAL ENTITY **RFC201000277: 1/29/10**
RFC201000278: 1/29/10

DATE ACCEPTED BY REGIONAL ENTITY **RFC201000277: 3/1/10**
RFC201000278: 3/1/10

DATE APPROVED BY NERC **RFC201000277: 3/24/10**
RFC201000278: 3/24/10

DATE PROVIDED TO FERC **RFC201000277: 3/24/10**
RFC201000278: 3/24/10

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **RFC201000277: 11/29/10**
RFC201000278: 6/30/10

EXTENSIONS GRANTED **N/A**

ACTUAL COMPLETION DATE **RFC201000277: 11/1/10**
RFC201000278: 6/30/10

DATE OF CERTIFICATION LETTER **RFC201000277:12/23/10**
RFC201000278: 6/30/10

CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF
RFC201000277: 11/1/10
RFC201000278: 6/30/10

DATE OF VERIFICATION LETTER **RFC201000277: 2/1/11**
RFC201000278: 2/3/11

VERIFIED COMPLETE BY REGIONAL ENTITY AS OF
RFC201000277: 11/1/10
RFC201000278: 6/30/10

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

RFC201000277

- **URE created a document to detail compliance requirements for the Standard. This action was completed on February 28, 2010.**
- **URE signed an agreement with its vendor stating the version upgrade to its software will resolve issues. This action was completed on April 15, 2010.**
- **URE validated the functionality of its non-production environment. This action was completed on July 15, 2010.**
- **URE upgraded its control system software. This action was completed on October 2, 2010.**
- **URE validated the functionality of its production environment. This action was completed on November 29, 2010.**

RFC201000278

- **URE received a statement of work from its vendor detailing actions to fix its database. This action was completed on February 26, 2010.**
- **URE scheduled the vendor's onsite support date to occur during a planned outage in April 2010. This action was completed on March 15, 2010.**
- **URE implemented actions to fix its database. This action was completed on April 30, 2010.**
- **URE validated the functionality of its production environment. This action was completed on June 30, 2010.**

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

RFC201000277

- **Screenshot verifying default user account administrator has been renamed to local-admin, undated**
- **Screenshot verifying user account password requirements (e.g. complexity and password age), undated**

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

- **Screenshot of event log showing successful modification of local-admin user account, dated November 1, 2010**
- **Screenshot of event log showing successful password change for local-admin user account, dated November 1, 2010**

RFC201000278

- **E-mail verifying functionality, dated April 21, 2010**
- **Screenshot of first time login, dated June 29, 2010**
- **Screenshot of password reset, dated June 29, 2010**
- **Screenshot of successful login after reset, dated June 29, 2010**
- **Screenshot of login with new password, dated June 29, 2010**
- **Screenshot of successful login, dated June 29, 2010**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R5.2.1

URE's Self-Report for CIP-007-1 R5.2.3

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2400 for CIP-007-1 R5.2.1

URE's Mitigation Plan MIT-10-2401 for CIP-007-1 R5.2.3

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-007-1 R5.2.1

URE's Certification of Mitigation Plan Completion for CIP-007-1 R5.2.3

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 R5.2.1

Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 R5.2.3