



NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

June 29, 2011

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations¹ discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Document (Attachment e), in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).²

This NOP is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the violations of CIP-002-1³ Requirement (R) 2, CIP-003-2 R1 and CIP-007-1 R6 . According to the Settlement Agreement,

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).

³ The Settlement Agreement and supporting documents for the CIP-002 violation refer to the violation as CIP-002-2 R1, instead of CIP-002-1 R1. The violation was discovered after Version 2 became enforceable but the violation was mitigated prior to Version 2 taking effect; therefore, the correct version of the standard related to this violation is CIP-002-1.

NERC Notice of Penalty
 Unidentified Registered Entity
 FROM THIS PUBLIC VERSION
 June 29, 2011
 Page 2

PRIVILEGED AND CONFIDENTIAL
 INFORMATION HAS BEEN REMOVED

URE neither admits nor denies the violations, but has agreed to the assessed penalty of ten thousand dollars (\$10,000), 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 RFC201000385, RFC201000386 and RFC201000303 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 January 4, 2011, by and between ReliabilityFirst and URE. The details of the findings and the basis for the penalty are set forth in the Disposition Document. 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-772	RFC201000385	CIP-002-1	2	High	6/30/08 – 3/16/10	10,000
	RFC201000386	CIP-003-2	1	Medium ⁴	4/1/10 – 5/18/10	
	RFC201000303	CIP-007-1	6	Lower ⁵	7/1/09 – 3/29/10	

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

CIP-002-1 R2 - OVERVIEW

After conducting a CIP Spot Check on URE (Spot Check), ReliabilityFirst determined that URE did not document the assessment of three generators to determine whether they were Critical Cyber Assets (CCAs), as required by the Standard.

CIP-003-2 R1 - OVERVIEW

After conducting the Spot Check, ReliabilityFirst determined that URE did not remove the exception for “acceptance of the risk” from its Cyber Security Policy, as required by the Standard.

⁴ CIP-003-2 R1 is assigned a Medium Violation Risk Factors (VRFs) and CIP-003-2 R1.1, R1.2 and R1.3 each are assigned a Medium VRF.

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

CIP-007-1 R6 - OVERVIEW

As a result of a Self-Report, ReliabilityFirst determined that URE did not produce and retain all logs specified in CIP-007-1 R6 for ninety days, and did not review and maintain records documenting its review of logs of system events related to cyber security, as required by the Standard.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed⁶

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,⁷ the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on May 9, 2011. The NERC BOTCC approved the Settlement Agreement, including ReliabilityFirst's assessment of a ten thousand dollar (\$10,000) 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 violations of the subject NERC Reliability Standards;
2. URE self-reported the violation of CIP-007-1 R6;
3. ReliabilityFirst reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor, as discussed in the Disposition Documents;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. ReliabilityFirst 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. ReliabilityFirst reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

⁶ See 18 C.F.R. § 39.7(d)(4).

⁷ *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).

NERC Notice of Penalty
Unidentified Registered Entity
FROM THIS PUBLIC VERSION
June 29, 2011
Page 4

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of ten thousand dollars (\$10,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

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

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

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

Attachments to be included as Part of this Notice of Penalty

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

- a) Settlement Agreement by and between ReliabilityFirst and URE executed January 4, 2011, included as Attachment a;
 - i. URE's Mitigation Plan MIT-10-2803 for CIP-007-1 R6, included as Attachment A to the Settlement Agreement;
 - ii. URE's Certification of Mitigation Plan Completion, included as Attachment B to the Settlement Agreement;
 - iii. ReliabilityFirst's Verification of Mitigation Plan Completion, included as Attachment C to the Settlement Agreement;
 - iv. URE's Mitigation Plan MIT-09-3186 for CIP-002-1 R2, included as Attachment D to the Settlement Agreement; and
 - v. URE's Mitigation Plan MIT-09-3187 for CIP-003-2 R1, included as Attachment E to the Settlement Agreement.
- b) Record Documents for CIP-002-1 R2:

- i. ReliabilityFirst's Spot Check, included as Attachment b-1;
 - ii. URE's Certification of Mitigation Plan Completion, included as Attachment b-2; and
 - iii. ReliabilityFirst's Verification of Mitigation Plan Completion, included as Attachment b-3.
- c) Record Documents for CIP-003-2 R1:
- i. ReliabilityFirst's Spot Check, included as Attachment c-1;
 - ii. URE's Certification of Mitigation Plan Completion, included as Attachment c-2; and
 - iii. ReliabilityFirst's Verification of Mitigation Plan Completion, included as Attachment c-3.
- d) Record Documents for CIP-007-1 R6:
- i. URE's Self-Report, included as Attachment d-1;
- e) Common Disposition Document, included as Attachment e;
- i. Disposition Document for CIP-002-2 R2, included as Attachment e-1;
 - ii. Disposition Document for CIP-003-2 R1, included as Attachment e-2; and
 - iii. Disposition Document for CIP-007-1 R6, included as Attachment e-3.

A Form of Notice Suitable for Publication⁸

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

⁸ See 18 C.F.R. § 39.7(d)(6).

NERC Notice of Penalty
Unidentified Registered Entity
FROM THIS PUBLIC VERSION
June 29, 2011
Page 6

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED

Notices and Communications

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

<p>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</p> <p>*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.</p>	<p>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</p> <p>Robert K. Wargo* Director of Enforcement and Regulatory Affairs ReliabilityFirst Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 bob.wargo@rfirst.org</p> <p>L. Jason Blake* Managing Enforcement Attorney ReliabilityFirst Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 jason.blake@rfirst.org</p> <p>Megan E. Gambrel* Associate Attorney 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 megan.gambrel@rfirst.org</p>
--	---

NERC Notice of Penalty
Unidentified Registered Entity
FROM THIS PUBLIC VERSION
June 29, 2011
Page 7

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED

Conclusion

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

Respectfully submitted,

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

/s/ Rebecca J. Michael
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

Attachment e

Common Disposition Document

DISPOSITION OF VIOLATION¹
INFORMATION COMMON TO INSTANT VIOLATIONS

Dated May 9, 2011

REGISTERED ENTITY

NERC REGISTRY ID

NOC#

**Unidentified Registered Entity
(URE)**

NCRXXXXX

NOC-772

REGIONAL ENTITY

ReliabilityFirst Corporation (ReliabilityFirst)

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 **\$10,000** FOR **THREE** 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.

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

**ReliabilityFirst considered URE's ICP a mitigating factor in
determining the penalty.**

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

See above.

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

YES NO
IF YES, EXPLAIN

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

YES NO
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES NO
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES NO
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES NO
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

NOTICE OF ALLEGED VIOLATION AND PROPOSED PENALTY OR
SANCTION ISSUED

DATE: OR N/A

SETTLEMENT REQUEST DATE

DATE: 11/15/10 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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL
INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment b

OUTCOME
APPEAL REQUESTED

Disposition Document for CIP-002-2 R2

DISPOSITION OF VIOLATION

Dated May 9, 2011

NERC TRACKING NO. **RFC201000385** REGIONAL ENTITY TRACKING NO. **RFC201000385**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-002-1¹	2		High	N/A

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 R2 provides: “Critical Asset Identification — The Responsible Entity^[2] shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.”

(Footnote added).

VIOLATION DESCRIPTION

ReliabilityFirst conducted a CIP Spot Check (Spot Check) of URE. During the Spot Check, ReliabilityFirst determined that URE was in violation of CIP-002-1 R2 for its failure to document the assessment of three generators to determine whether they were Critical Assets.

¹ The Settlement Agreement and supporting documents for the CIP-002 violation refer to the violation as CIP-002-2 R1, instead of CIP-002-1 R1. The violation was discovered after Version 2 became enforceable but the violation was mitigated prior to Version 2 taking effect; therefore, the correct version of the standard related to this violation is CIP-002-1.

² Within the text of Standard CIP-002, “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.

URE's procedure for assessment and identification of Critical Assets requires URE to identify, in its asset assessment worksheet, all bulk electric system assets. Despite this documented procedure, URE identified the three generators as assets, but did not apply its Risk Based Assessment Methodology (RBAM) to the three generators or document its assessment of whether the three generators were Critical Assets.

URE applied its RBAM to the three generators, and determined that the three generators were non-critical. In this instance, ReliabilityFirst agreed that the three generators were non-Critical Assets.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

ReliabilityFirst determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the violation was a documentation error that did not affect the outcome of URE's Critical Asset determination, as URE correctly identified all of its Critical Assets as such and the referenced three generators were not deemed critical.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) 6/30/09 (date URE was required to be Compliant with Standard) through 3/16/10 (Mitigation Plan completion)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY Spot Check

IS THE VIOLATION STILL OCCURRING YES NO
IF YES, EXPLAIN

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	MIT-09-3186
DATE SUBMITTED TO REGIONAL ENTITY	11/15/10
DATE ACCEPTED BY REGIONAL ENTITY	12/16/10
DATE APPROVED BY NERC	12/30/10
DATE PROVIDED TO FERC	1/5/11

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

N/A

MITIGATION PLAN COMPLETED YES NO

EXPECTED COMPLETION DATE **Submitted as complete**

EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **3/16/10**

DATE OF CERTIFICATION LETTER **1/4/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **3/16/10**

DATE OF VERIFICATION LETTER **2/16/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **3/16/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

- **On March 16, 2010, URE revised the procedure for assessment and identification of Critical Assets to include changes that comply with the Reliability Standard.**

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)

- **Procedure for assessment and identification of Critical Assets**

EXHIBITS:

SOURCE DOCUMENT

ReliabilityFirst's Spot Check

MITIGATION PLAN

URE's Mitigation Plan MIT-09-3186

CERTIFICATION BY REGISTERED ENTITY

URE's Certification of Mitigation Plan Completion

VERIFICATION BY REGIONAL ENTITY

ReliabilityFirst's Verification of Mitigation Plan Completion

Disposition Document for CIP-003-2 R1

DISPOSITION OF VIOLATION

Dated May 9, 2011

NERC TRACKING NO. **RFC201000386** REGIONAL ENTITY TRACKING NO. **RFC201000386**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-003-2	1		Medium¹	Severe²

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

The purpose statement of CIP-003-2 provides: “Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.”

CIP-003-2 R1 provides:

- R1. Cyber Security Policy — The Responsible Entity^[3] shall document and implement a cyber security policy that represents management’s commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:**
 - R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.**
 - R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.**

¹ CIP-003-2 R1 is assigned a Medium Violation Risk Factors (VRFs) and CIP-003-2 R1.1, R1.2 and R1.3 each are assigned a Medium VRF.

² On December 18, 2009, NERC submitted revised Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for CIP-002-2 through CIP-009-2. On June 20, 2011, FERC issued an order approving the Version 2 VRFs and VSLs and made them effective on April 1, 2010, the date the Version 2 CIP Reliability Standards became effective.

³ Within the text of Standard CIP-003, “Responsible Entity” shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

(Footnote added).

VIOLATION DESCRIPTION

ReliabilityFirst conducted a CIP Spot Check (Spot Check) of URE. During the Spot Check, ReliabilityFirst discovered that URE did not remove the term “acceptance of the risk” from its Cyber Security Policy.

One of the modifications made to CIP-003-1 when CIP-003-2 took effect on April 1, 2010 was the removal of the term “statement accepting risk” from the Standard. As a result of that change, acceptance of the risk is no longer an allowable exception for non-conformance with a Cyber Security Policy. URE, however, failed to remove the acceptance of the risk exception from its Cyber Security Policy in accordance with this change to the CIP-003 Standard.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

ReliabilityFirst determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the violation was a documentation issue that did not substantively affect URE’s Cyber Security Policy; none of URE’s identified and approved exceptions to its Cyber Security Policy were based on acceptance of risk. In addition, URE did not identify any exceptions to its Cyber Security Policy during the audit period.

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) 4/1/10 (when URE was required to be compliant with the Standard) through 5/18/10 (Mitigation Plan completion)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY Spot Check

IS THE VIOLATION STILL OCCURRING YES NO
IF YES, EXPLAIN

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **MIT-09-3187**
DATE SUBMITTED TO REGIONAL ENTITY **11/15/10**
DATE ACCEPTED BY REGIONAL ENTITY **12/16/10**
DATE APPROVED BY NERC **12/30/10**
DATE PROVIDED TO FERC **1/5/11**

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

N/A

MITIGATION PLAN COMPLETED YES NO

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

DATE OF CERTIFICATION LETTER **1/4/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **5/18/10**

DATE OF VERIFICATION LETTER **2/16/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **5/18/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

- **URE removed the “acceptance of risk” exception from its Cyber Security Policy. This action was completed on May 18, 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)

- **URE’s Cyber Security Policy**

EXHIBITS:

SOURCE DOCUMENT

ReliabilityFirst's Spot Check

MITIGATION PLAN

URE's Mitigation Plan MIT-09-3187

CERTIFICATION BY REGISTERED ENTITY

URE's Certification of Mitigation Plan Completion

VERIFICATION BY REGIONAL ENTITY

ReliabilityFirst's Verification of Mitigation Plan Completion

Disposition Document for CIP-007-1 R6

DISPOSITION OF VIOLATION

Dated May 9, 2011

NERC TRACKING NO. **RFC201000303** REGIONAL ENTITY TRACKING NO. **RFC201000303**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	6	6.4, 6.5	Lower¹	N/A²

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

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

Standard CIP-007 requires Responsible Entities 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 provides, in pertinent part:

R6. Security Status Monitoring — The Responsible Entity^[3] shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

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

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

² At the time of the violation, no VSLs were in effect for CIP-007-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

³ 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.

R6.5 The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

(Footnote added).

VIOLATION DESCRIPTION

URE submitted a Self-Report to ReliabilityFirst concerning a violation of CIP-007-1 R6 for failure to produce and retain all logs specified in CIP-007-1 R6 for ninety days, and for failure to review and maintain records documenting its review of logs of system events related to cyber security.

URE reported that 47 of its terminal servers (40 of which were deemed Critical Cyber Assets (CCAs)) did not retain security logs for longer than 14 days, thereby violating CIP-007-1 R6.4. In addition, URE could not provide evidence that it reviewed the logs for the 40 terminal servers deemed CCAs, thereby violating CIP-007-1 R6.5. For the remaining seven terminal servers deemed non-CCAs, URE was not completing security event logging, in violation of CIP-007-1 R6.4 and R6.5.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

ReliabilityFirst determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the terminal servers in question are enclosed within a well-managed physical and electronic security perimeter. In addition, URE has assessment, training, and awareness programs, as well as operational procedures for its personnel to minimize the risk related to personnel who are authorized to access CIP devices. An unauthorized change in the devices would have been detected by URE personnel because any changes to the terminal server physical port configuration would have disrupted application communication with the devices. This would have resulted in immediate application alarms to SCADA operators related to the disrupted communication. Finally, seven of the devices are unrelated to the reliability of the bulk power system because those devices communicate with devices used for natural gas. In addition, URE prevents these devices and electric devices from interacting within the electronic security perimeter.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) **7/1/09 (date URE was required to be compliant with Standard) through 3/29/10 (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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	MIT-10-2803
DATE SUBMITTED TO REGIONAL ENTITY	8/26/10
DATE ACCEPTED BY REGIONAL ENTITY	9/2/10
DATE APPROVED BY NERC	9/8/10
DATE PROVIDED TO FERC	9/8/10

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	3/29/10

DATE OF CERTIFICATION LETTER	9/22/10
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	3/29/10

DATE OF VERIFICATION LETTER **10/15/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **3/29/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT
RECURRENCE

- **URE wrote the login, logout, and failed login attempts for 34 terminal servers to a security event log that can retain information for at least 90 days and can be reviewed regularly by its Security personnel. This action was completed on March 26, 2010.**
- **URE wrote the login and logout traps for its 7 remaining terminal servers to a security event log that can retain information for at least 90 days and can be reviewed regularly by its Security personnel. This action was completed on March 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)

- **Documents showing that the terminal servers can retain information for at least 90 days and that the Security personnel are able to regularly review this information.**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2803

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

VERIFICATION BY REGIONAL ENTITY
ReliabilityFirst's Verification of Mitigation Plan Completion