**PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

February 23, 2011

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

**Re: NERC Abbreviated Notice of Penalty regarding Unidentified Registered 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 violation[1] discussed in detail in the Settlement Agreement (Attachment c) and the Disposition Document (Attachment d), 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 enforceable violations of PRC-005-1 Requirement (R) 2/R2.1, two violations of CIP-004-1 R4, CIP-004-1 R2, two violations of CIP-004-1 R3, CIP-007-1 R1/R1.1, CIP-008-1 R1, EOP-001-0 R6, PRC-005-1 R1, FAC-009-1 R1, FAC-014-1 R2 and R4, TPL-002-0 R1, TPL-003-0 R1 and CIP-003-1 R4. According to the Settlement Agreement, URE stipulates to the facts of the Settlement Agreement and admits that the stipulated facts constitute violations and has agreed to the assessed penalty of

[1] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

[2] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2010). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

one hundred thousand dollars ($100,000), 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 RFC200800079, RFC200900125, RFC200900135, RFC200900198, RFC200900136, RFC200900197, RFC200900137, RFC200900138, RFC200900148, RFC200900149, RFC200900150, RFC200900151, RFC200900152, RFC200900153, RFC200900154, and RFC201000236 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 June 28, 2010, 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-594 | RFC200800079 | PRC-005-1 | 2/2.1 | High[3] | 4/24/08-9/30/08 | 100,000 |
| | RFC200900125 | CIP-004-1 | 4 | Medium[4] | 7/1/08-7/1/09 | |
| | RFC200900135 | CIP-004-1 | 2 | Medium[5] | 7/1/08-7/1/09 | |
| | RFC200900136 | CIP-004-1 | 3 | Medium[6] | 7/1/08-7/1/09 | |

[3] PRC-005-1 R2 has a Lower Violation Risk Factor (VRF); R2.1 and R2.2 each have a High VRF. During a final review of the standards subsequent to the March 23, 2007 filing of the Version 1 VRFs, NERC identified that some standards requirements were missing VRFs; one of these include PRC-005-1 R2.1. On May 4, 2007, NERC assigned PRC-005 R2.1 a High VRF. In the Commission's June 26, 2007 Order on Violation Risk Factors, the Commission approved the PRC-005-1 R2.1 "High" VRF as filed. Therefore, the High VRF was in effect from June 26, 2007.

[4] When NERC filed VRFs it originally assigned CIP-004-1 R4.2 as a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R4.2 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[5] When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

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

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

| NOC ID | NERC Violation ID | Reliability Std. | Req. (R) | VRF | Duration | Total Penalty ($) |
|---|---|---|---|---|---|---|
| | RFC200900197 | CIP-004-1 | 3 | Medium[7] | 8/13/09-10/1/09 | |
| | RFC200900198 | CIP-004-1 | 4/4.1 | Lower | 7/21/09-10/1/09 | |
| | RFC200900137 | CIP-007-1 | 1/1.1 | Medium[8] | 7/1/08-4/27/09 | |
| | RFC200900138 | CIP-008-1 | 1 | Lower | 7/1/08-4/24/09 | |
| | RFC200900148 | EOP-001-0 | 6 | Medium | 6/18/07-8/4/09 | |
| | RFC200900149 | PRC-005-1 | 1 | High[9] | 6/18/07-8/26/09 | |
| | RFC200900150 | FAC-009-1 | 1 | Medium | 6/18/07-8/24/09 | |
| | RFC200900151 | FAC-014-1[10] | 2 | Medium | 1/1/09-6/30/09 | |
| | RFC200900152 | FAC-014-1[11] | 4 | Medium | 1/1/09-6/30/09 | |
| | RFC200900153 | TPL-002-0 | 1 | High[12] | 6/18/07-11/13/09 | |
| | RFC200900154 | TPL-003-0 | 1 | High[13] | 6/18/07-11/13/09 | |
| | RFC201000236 | CIP-003-1[14] | 4 | Medium[15] | 10/5/09-2/1/10 | |

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

[7] *Id*.
[8] CIP-007-1 R1 and R1.1 each have a Medium VRF; R1.2 and R1.3 each have a Lower VRF.
[9] When NERC filed VRFs it originally assigned PRC-005-1 R1 a Medium VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on August 9, 2007, the Commission approved the modified High VRF. Therefore, the Medium VRF for PRC-005-1 R1 was in effect from June 18, 2007 until August 9, 2007 when the High VRF became effective.
[10] FAC-014-1 was enforceable from January 1, 2009 through April 28, 2009. FAC-014-2 is the current enforceable Standard as of April 29, 2009.
[11] *Id*.
[12] TPL-002-1 R1 has a High VRF and its sub-requirements have Medium VRFs. When NERC filed VRFs it originally assigned TPL-002-0 R1 a Medium VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on August 9, 2007, the Commission approved the modified High VRF. Therefore, the Medium VRF for TPL-002-0 R1 was in effect from June 18, 2007 until August 9, 2007 when the High VRF became effective.
[13] TPL-003-1 R1 has a High VRF and its sub-requirements have Medium VRFs.
[14] CIP-003-1 was enforceable from July 1, 2008 for Table 1 entities with Critical Cyber Assets in its System Control Center through March 31, 2010. CIP-003-2 is the current enforceable Standard as of April 1, 2010.
[15] CIP-003-1 R4 and R4.1 have a Medium VRF; R4.2 and R4.3 each have a Lower VRF.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRC-005-1 R2/R2.1 - OVERVIEW

On September 16, 2008, URE self-reported a violation of PRC-005-1 R2, specifically R2.1. Reliability*First* determined that URE, as a Generator Owner that owns a generation Protection System,[16] did not provide evidence that two of its seven batteries (28.6%) were maintained and tested in the second quarter of 2008 as required by URE's Protection System Maintenance and Testing Program.

CIP-004-1 R4 (RFC200900125), CIP-004-1 R2 (RFC200900135) and CIP-004-1 R3 (RFC200900136) - OVERVIEW

On February 27, 2009, URE self-reported a violation of CIP-004-1 R4, specifically R4.2. On April 24, 2009, URE amended its self-report to include a violation of R4.1. Reliability*First* determined that URE did not: (a) revoke access within seven calendar days for personnel who did not complete training and personal risk assessment (PRA) within the seven calendar days from the effective date of the Standard; (b) revoke access within seven calendar days for personnel who did not require access to Critical Cyber Assets; (c) have a comprehensive list of all personnel with access;[17] (d) conduct quarterly reviews of a complete access list in the third quarter of 2008 and the first quarter of 2009; or (e) perform a quarterly review in the fourth quarter of 2008.

In its April 24, 2009 amended Self-Report, URE also self-reported a violation of CIP-004-1 R2, specifically R2.1 and R2.3. Reliability*First* determined that URE did not ensure that all personnel with access to Critical Cyber Assets were trained within 90 days of being granted that access and URE failed to maintain documentation of annual training for 47 out of 83 personnel.

In its April 24, 2009 amended Self-Report, URE also self-reported a violation of CIP-004-1 R3, specifically R3.1 and R3.3. Reliability*First* determined that URE did not conduct PRAs for 21 of its 83 employees, contractors and service providers who had authorized cyber or authorized unescorted physical access within 30 days of the employees, contractors and service providers being granted such access.

CIP-004-1 R3 (RFC200900197) and CIP-004-1 R4/R4.1 (RFC200900198) - OVERVIEW[18]

On September 16, 2009, URE self-reported violations of CIP-004-1 R3 and R4, specifically R4.1. Reliability*First* determined that URE did not ensure that it had a completed PRA on file within 30 days of unintentionally granting a contract worker unescorted physical access to Critical Cyber Assets as required by R3. Reliability*First* also determined that URE did not update its master list of personnel with authorized cyber or unescorted physical access rights to a Critical Cyber Asset within seven days of granting access to the contract employee as required by R4.1.

---

[16] *The NERC Glossary of Terms Used in Reliability Standards* defines Protection System as "Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry."

[17] URE had a list of employees with physical access, which was generated from their physical access software system, but that list did not include individuals with cyber access or contractors or service providers with physical access.

[18] For purposes of penalty determination, Reliability*First* considered URE's second violation of CIP-004-1, R3 (RFC200900197) and of CIP-004-1 R4 (RFC200900198) to be an aggravating factor

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

CIP-007-1 R1 - OVERVIEW

On April 24, 2009, URE self-reported a violation of CIP-007-1 R1. Reliability*First* determined that URE did not create cyber security test procedures which are required to minimize the adverse effects of new cyber assets and significant changes to existing cyber assets.

CIP-008-1 R1 - OVERVIEW

On April 24, 2009, URE self-reported a violation of CIP-008-1 R1. Reliability*First* determined that URE's cyber security incident response plan, did not address URE's process for updating the cyber security incident response plan (Plan) within 90 calendar days of any changes, ensuring that the Plan is reviewed at least annually, and ensuring that the Plan is tested at least annually.

EOP-001-0 R6- OVERVIEW

In preparation for an upcoming audit (Audit), URE self-reported a violation of EOP-001-0 R6 on May 14, 2009. Reliability*First* determined that URE did not provide a copy of its updated emergency plans to its neighboring Transmission Operators and Balancing Authorities in 2007.

PRC-005-1 R1 - OVERVIEW

On April 24, 2009, in preparation of the Audit, URE self-reported a violation of PRC-005-1 R1. Reliability*First* determined that URE, did not have a basis for the maintenance and testing intervals or a summary of maintenance and testing procedures in its Protection System Maintenance and Testing Program for 19 out of 244 (7.8%) of its DC Control Circuitry devices.

FAC-009-1 R1 - OVERVIEW

During the Audit, Reliability*First* determined that URE did not establish Facility Ratings that were consistent with its Facility Ratings Methodology.

FAC-014-1 R2 and R4 - OVERVIEW

During the Audit, Reliability*First* determined that URE did not establish System Operating Limits (SOLs) as directed by its Reliability Coordinator for URE's portion of the Reliability Coordinator Area that were consistent with the Reliability Coordinator's SOL Methodology as required by R2. During the Audit, Reliability*First* also determined that URE did not establish SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Transmission Planning Area that were consistent with the Reliability Coordinator's SOL Methodology as required by R4.

TPL-002-0 R1 - OVERVIEW

During the Audit, Reliability*First* determined that URE did not demonstrate system performance was within limits (system stable) via dynamic studies or simulations for Category B contingencies.

TPL-003-0 R1 - OVERVIEW

During the Audit, Reliability*First* determined that URE did not demonstrate that system performance met Category C contingencies.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

CIP-003-1 R4 - OVERVIEW

On February 1, 2010, URE self-reported a violation of CIP-003-1 R4. Reliability*First* determined that URE did not classify information associated with Critical Cyber Assets based on the sensitivity of the Critical Cyber Asset information.

**Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed**[19]

**Basis for Determination**

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines, the Commission's July 3, 2008 and October 26, 2009 Guidance Orders,[20] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on September 10, 2010. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of a one hundred thousand dollar ($100,000) 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 with the exception of the repeat violations of CIP-004-1 R3 and R4;[21]
2. URE self-reported 11 of the 16 violations, although one of the self-reported violations was reported in preparation of a self-certification, one violation was reported in preparation of the Audit, and another was initially self-reported but expanded by the Audit;
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, as discussed in the Disposition Documents which Reliability*First* considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

[19] *See* 18 C.F.R. § 39.7(d)(4).

[20] *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).

[21] For purposes of penalty determination, Reliability*First* considered URE's second violations of CIP-004-1, R3 (RFC200900197) and CIP-004-1, R4 (RFC200900198) to be an aggravating factor because the violations were not related to a single act or common incidence of non-compliance.

Reliability*First* determined the violations of CIP-004-1 R3 and R4/R4.1 (RFC200900197 and RFC200900198), which were submitted in the same September 16, 2009 Self Report, were "related to a single act or common incidence of non-compliance" for which Reliability*First* would assess "a single aggregate penalty."

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

6. Reliability*First* determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed in the Disposition Documents; and
7. Reliability*First* reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approves the Settlement Agreement and believes that the assessed penalty of one hundred thousand dollars ($100,000) 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 Notice of Penalty include privileged and 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. Specifically, this includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business and confidential information exempt from the mandatory public disclosure requirements of the Freedom of Information Act, 5 U.S.C. 552, and should be withheld from public disclosure.

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) URE's Narrative Supplement to Reliability*First* Violation Self Reporting Form for CIP-004-1 R4 (RFC200900125), CIP-004-1 R2 (RFC200900135), CIP-004-1 R3 (RFC200900136), CIP-007-1 R1, CIP-008-1 R1 and PRC-005-1 R1 dated April 24, 2009, included as Attachment a;

b) Reliability*First*'s Public Compliance Audit Report for FAC-009-1 R1, FAC-014-1 R2 and R4, TPL-002-0 R1 and TPL-003-0 R1, included as Attachment b;[22]

[22] The audit report also lists violations of CIP-001-1 R2, EOP-008-0 R1 and PRC-004-1 R3. Reliability*First* determined there was insufficient basis to proceed with a violation of EOP-008-0, R1 and CIP-001-1, R2, and did

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

c) Settlement Agreement by and between Reliability*First* and URE executed June 28, 2010, included as Attachment c;

1. URE's Mitigation Plan, MIT-08-1110, for PRC-005-1 R2.1 dated September 17, 2008, included as Attachment a to the Settlement Agreement;
2. URE's Certification of Mitigation Plan Completion for PRC-005-1 R2.1 dated October 21, 2008, included as Attachment b to the Settlement Agreement;
3. URE's Mitigation Plan, MIT-08-2311, for CIP-004-1 R4, R2, R3, R3 and R4.1 dated January 20, 2010, included as Attachment c to the Settlement Agreement;
4. URE's Certification of Mitigation Plan Completion for CIP-004-1 R4, R2, R3, R3 and R4.1 dated February 12, 2010, included as Attachment d to the Settlement Agreement;
5. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R4, R2, R3, R3 and R4.1 dated April 5, 2010, included as Attachment e to the Settlement Agreement;
6. URE's Mitigation Plan, MIT-08-1985, for CIP-007-1 R1 dated September 4, 2009, included as Attachment f to the Settlement Agreement;
7. URE's Certification of Mitigation Plan Completion for CIP-007-1 R1 dated September 28, 2009 and submitted September 29, 2009, included as Attachment g to the Settlement Agreement;
8. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 R1 dated October 27, 2009, included as Attachment h to the Settlement Agreement;
9. URE's Mitigation Plan, MIT-08-1986, for CIP-008-1 R1 dated September 4, 2009, included as Attachment i to the Settlement Agreement;
10. URE's Certification of Mitigation Plan Completion for CIP-008-1 R1 dated September 28, 2009 and submitted on September 29, 2009, included as Attachment j to the Settlement Agreement;
11. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-008-1 R1 dated October 7, 2009, included as Attachment k to the Settlement Agreement;
12. URE's Mitigation Plan, MIT-09-2050, for EOP-001-0 R6 dated September 28, 2009, included as Attachment l to the Settlement Agreement;
13. URE's Certification of Mitigation Plan Completion for EOP-001-0 R6 submitted November 20, 2009, included as Attachment m to the Settlement Agreement;
14. Reliability*First*'s Verification of Mitigation Plan Completion for EOP-001-0 R6 dated December 2, 2009, included as Attachment n to the Settlement Agreement;
15. URE's Mitigation Plan, MIT-07-2562, for PRC-005-1 R1 dated June 10, 2010, included as Attachment o to the Settlement Agreement;

---

not include the possible violation of PRC-004-1, R3 in this settlement agreement, but notes that it has been fully mitigated.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

16. URE's Mitigation Plan, MIT-07-2551, for FAC-009-1 R1dated May 21, 2010, included as Attachment p to the Settlement Agreement;
17. URE's Certification of Mitigation Plan Completion for FAC-009-1 R1 dated June 2, 2010, included as Attachment q to the Settlement Agreement;
18. URE's Mitigation Plan, MIT-09-2549, for FAC-014-1 R2 and R4 dated May 21, 2010, included as Attachment r to the Settlement Agreement;
19. URE's Certification of Mitigation Plan Completion for FAC-014-1 R2 and R4 dated June 2, 2010, included as Attachment s to the Settlement Agreement;
20. URE's Mitigation Plan, MIT-07-2552, for TPL-002-0 R1 dated May 27, 2010, included as Attachment t to the Settlement Agreement;
21. URE's Certification of Mitigation Plan Completion for TPL-002-0 R1 submitted June 2, 2010, included as Attachment u to the Settlement Agreement;
22. URE's Mitigation Plan, MIT-07-2553, for TPL-003-0 R1 dated May 27, 2010, included as Attachment v to the Settlement Agreement;
23. URE's Certification of Mitigation Plan Completion for TPL-003-0 R1 submitted June 2, 2010, included as Attachment w to the Settlement Agreement;
24. URE's Mitigation Plan, MIT-10-2563, for CIP-003-1 R4 dated June 10, 2010, included as Attachment x to the Settlement Agreement;

d) Disposition Document for Common Information dated September 10, 2010 included as Attachment d;

1. Disposition Document for PRC-005-1 R2.1 included as Attachment d-1;
2. Disposition Document for CIP-004-1 R4, R2, R3, R3 and R4.1 included as Attachment d-2;
3. Disposition Document for CIP-007-1 R1 included as Attachment d-3;
4. Disposition Document for CIP-008-1 R1 included as Attachment d-4;
5. Disposition Document for EOP-001-0 R6 included as Attachment d-5;
6. Disposition Document for PRC-005-1 R1 included as Attachment d-6;
7. Disposition Document for FAC-009-1 R1 included as Attachment d-7;
8. Disposition Document for FAC-014-1 R2 and R4 included as Attachment d-8;
9. Disposition Document for TPL-002-0 R1 included as Attachment d-9;
10. Disposition Document for TPL-003-0 R1 included as Attachment d-10;
11. Disposition Document for CIP-003-1 R4 included as Attachment d-11;

e) Additional Record documents for PRC-005-1 R2.1 included as Attachment e:

1. URE's Self-Report dated September 16, 2008;
2. URE's Self-Certification dated September 23, 2008;

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

3. Reliability*First*'s Verification of Mitigation Plan Completion dated June 11, 2010;

f) Additional Record documents for CIP-004-1 R4, R2, R3, R3 and R4.1 included as Attachment f:

1. URE's Self-Report CIP-004-1 R4 (RFC200900125) dated February 27, 2009;
2. URE's Self-Report for CIP-004-1 R4 (RFC200900125), CIP-004-1 R2 (RFC200900135) and CIP-004-1 R3 (RFC200900136) dated April 24, 2009;
3. URE's Narrative Supplement to Reliability*First* Violation Self Reporting Form dated April 24, 2009 (*see* Attachment a);
4. URE's Self-Report for CIP-004-1 R3 (RFC200900197) and CIP-004-1 R4.1 (RFC200900198) dated September 16, 2009;

g) Additional Record documents for CIP-007-1 R1 included as Attachment g:

1. URE's Self-Report dated April 24, 2009;
2. URE's Narrative Supplement to Reliability*First* Violation Self Reporting Form dated April 24, 2009 (*see* Attachment a);

h) Additional Record documents for CIP-008-1 R1 included as Attachment h:

1. URE's Self-Report dated April 24, 2009;
2. URE's Narrative Supplement to Reliability*First* Violation Self Reporting Form dated April 24, 2009 (*see* Attachment a);

i) Additional Record documents for EOP-001-0 R6 included as Attachment i:

1. URE's Self-Report dated May 14, 2009;

j) Additional Record documents for PRC-005-1 R1 included as Attachment j:

1. URE's Self-Report dated April 24, 2009;
2. URE's Narrative Supplement to Reliability*First* Violation Self Reporting Form dated April 24, 2009 (*see* Attachment a);
3. URE's Certification of Mitigation Plan Completion dated June 22, 2010;
4. Reliability*First*'s Verification of Mitigation Plan Completion, dated August 20, 2010;

k) Additional Record documents for FAC-009-1 R1 included as Attachment k:

1. Reliability*First*'s Public Audit Report (*see* Attachment b);
2. Reliability*First*'s Verification of Mitigation Plan Completion dated July 14, 2010;

l) Additional Record documents for FAC-014-1 R2 and R4 included as Attachment l:

1. Reliability*First*'s Public Audit Report (*see* Attachment b);
2. Reliability*First*'s Verification of Mitigation Plan Completion dated July 13, 2010;

m) Additional Record documents for TPL-002-0 R1 included as Attachment m:

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

1. Reliability*First*'s Public Audit Report (*see* Attachment b);
2. Reliability*First*'s Verification of Mitigation Plan Completion dated July 30, 2010;

n) Additional Record documents for TPL-003-0 R1 included as Attachment n:

1. Reliability*First*'s Public Audit Report (*see* Attachment b);
2. Reliability*First*'s Verification of Mitigation Plan Completion dated July 30, 2010;

o) Additional Record documents for CIP-003-1 R4 included as Attachment o:

1. URE's Self-Report dated February 1, 2010;
2. URE's Certification of Mitigation Plan Completion dated June 22, 2010; and
3. Reliability*First*'s Verification of Mitigation Plan Completion dated July 13, 2010.

**A Form of Notice Suitable for Publication**[23]

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

[23] *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<br>President and Chief Executive Officer<br>David N. Cook*<br>Sr. Vice President and General Counsel<br>North American Electric Reliability Corporation<br>116-390 Village Boulevard<br>Princeton, NJ 08540-5721<br>(609) 452-8060<br>(609) 452-9550 – facsimile<br>david.cook@nerc.net<br><br>Megan E. Gambrel*<br>Associate Attorney<br>ReliabilityFirst Corporation<br>320 Springside Drive, Suite 300<br>Akron, Ohio 44333<br>(330) 456-2488<br>(330) 456-5408 – facsimile<br>megan.gambrel@rfirst.org | Rebecca J. Michael*<br>Assistant General Counsel<br>Davis Smith*<br>Attorney<br>North American Electric Reliability Corporation<br>1120 G Street, N.W.<br>Suite 990<br>Washington, DC 20005-3801<br>(202) 393-3998<br>(202) 393-3955 – facsimile<br>rebecca.michael@nerc.net<br>davis.smith@nerc.net<br><br>L. Jason Blake*<br>Corporate Counsel<br>Reliability*First* Corporation<br>320 Springside Drive, Suite 300<br>Akron, OH 44333<br>(330) 456-2488<br>jason.blake@rfirst.org<br><br>Robert K. Wargo*<br>Director of Enforcement & Regulatory Affairs<br>Reliability*First* Corporation<br>320 Springside Drive, Suite 300<br>Akron, Ohio 44333<br>(330) 456-2488<br>(330) 456-5408 – facsimile<br>bob.wargo@rfirst.org<br><br>*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
Assistant General Counsel
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 d

# Disposition Document for Common Information dated September 10, 2010

# DISPOSITION OF VIOLATION[1]

**INFORMATION COMMON TO INSTANT VIOLATIONS**
**Dated September 10, 2010**

| REGISTERED ENTITY | NERC REGISTRY ID | NOC# |
|---|---|---|
| **Unidentified Registered Entity (URE)** | **NCRXXXXX** | **NOC-594** |

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 ☐

**URE stipulates to the facts contained in the Settlement Agreement and admits that the stipulated facts constitute violations.**

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 **$100,000** FOR **SIXTEEN (16)** VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST ANY CONFIRMED OR SETTLED 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.

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

LIST ANY PRIOR CONFIRMED OR SETTLED 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 URE's internal compliance program a mitigating factor in determining the penalty. At the time of the violation, URE had a documented internal compliance program.**

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

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

YES ☐ NO ☒
IF YES, EXPLAIN

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

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☒ NO ☐
IF YES, EXPLAIN
**Included in the Settlement Agreement are two violations of CIP-004-1 R3 (RFC200900136 and RFC200900197) and two violations of CIP-004-1 R4 (RFC200900125 and RFC200900198). For purposes of penalty determination, Reliability*First* considered URE's second violation of CIP-004-1, R3 and CIP-004-1 R4 (RFC200900198) to be an aggravating factor because the two sets of violations were not related to a single act or common incidence of non-compliance.**

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

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

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **9/4/09 and 5/28/10** OR N/A ☐

**URE requested settlement for RFC200800079 on September 4, 2009 and for the remaining violations on May 28, 2010.**

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

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

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

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for PRC-005-1 R2.1

# DISPOSITION OF VIOLATION
## Dated September 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC200800079** | **RFC200800079** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **PRC-005-1** | **2** | **2.1** | **High**[1] | **Moderate**[2] |

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

**The purpose statement of PRC-005-1 provides: "To ensure all transmission and generation Protection Systems[3] affecting the reliability of the Bulk Electric System (BES) are maintained and tested." (Footnote added)**

**PRC-005-1 R2 provides in pertinent part:**

> **R2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization[4] on request (within 30 calendar days). The documentation of the program implementation shall include:**
>
> > **R2.1. Evidence Protection System devices were maintained and tested within the defined intervals. …**

[1] PRC-005-1 R2 has a "Lower" Violation Risk Factor (VRF); R2.1 and R2.2 each have a "High" VRF. During a final review of the standards subsequent to the March 23, 2007 filing of the Version 1 VRFs, NERC identified that some standards requirements were missing VRFs; one of these include PRC-005-1 R2.1. On May 4, 2007, NERC assigned PRC-005 R2.1 a "High" VRF. In the Commission's June 26, 2007 Order on Violation Risk Factors, the Commission approved the PRC-005-1 R2.1 "High" VRF as filed. Therefore, the "High" VRF was in effect from June 26, 2007.

[2] The Self-Report incorrectly states a "High" VSL.

[3] *The NERC Glossary of Terms Used in Reliability Standards* defines Protection System as "Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry."

[4] Consistent with applicable FERC precedent, the term 'Regional Reliability Organization' in this context refers to Reliability*First*.

VIOLATION DESCRIPTION

**On September 16, 2008, URE self-reported a violation of PRC-005-1 R2.1 for failing to test (28.6%) of its batteries in the second quarter of 2008 as required by URE's Protection System Maintenance and Testing Program.**

**The two missed batteries were located at URE's one facility and relate to URE's failure to perform scheduled battery maintenance for its Units 2 and 3 batteries on April 24, 2008, as required for the second quarter. The Units 2 and 3 batteries each consist of 60 cells. Although URE's maintenance management system successfully produced the second quarter work orders, URE never scheduled the performance of the work.**

**The contractor who performed the first quarter testing on the batteries at issue reported that the voltages on five out of the 120 cells were slightly below the manufacturer's recommended range by 1.5%, but that the overall voltage of the batteries was sufficient for required system voltage. When URE performed the third quarter battery testing on September 10, 2008, the tests demonstrated that voltage levels were consistent with those identified during the first quarter test. URE did, however, identify one minor abnormality during the third quarter test, a broken battery cap.[5]**

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 because the one facility was performing weekly visual and connection checks on the batteries to assure the integrity of the batteries between quarterly tests. Additionally, when URE performed third quarter battery testing on September 10, 2008, the tests demonstrated that voltage levels were consistent with those identified during the first quarter test.**

[5] The broken battery cap was discovered during the third quarter battery maintenance on September 10, 2008, and corrected on September 16, 2008.

## II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

| | |
|---|---|
| SELF-REPORT | ☒[6] |
| SELF-CERTIFICATION | ☐ |
| COMPLIANCE AUDIT | ☐ |
| COMPLIANCE VIOLATION INVESTIGATION | ☐ |
| SPOT CHECK | ☐ |
| COMPLAINT | ☐ |
| PERIODIC DATA SUBMITTAL | ☐ |
| EXCEPTION REPORTING | ☐ |

DURATION DATE(S) **4/24/08 (the date of the missed battery testing interval for the two batteries) through 9/30/08 (the third quarter test date)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **9/16/08**[7]

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

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

## III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

| | |
|---|---|
| MITIGATION PLAN NO. | **MIT-08-1110** |
| DATE SUBMITTED TO REGIONAL ENTITY | **9/17/08 (signed 9/16/08)** |
| DATE ACCEPTED BY REGIONAL ENTITY | **9/24/08**[8] |
| DATE APPROVED BY NERC | **11/6/08** |
| DATE PROVIDED TO FERC | **11/6/08** |

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

---

[6] The method of discovery was by a self-report; however Reliability*First* considered that the self-report was submitted prior to a self-certification and determined the penalty accordingly (*i.e.* some mitigating credit but not as much as if the self-report was not made just prior to a self certification).
[7] The Mitigation Plan incorrectly states that the violation was discovered on September 9, 2008.
[8] The Settlement Agreement (page 26) incorrectly states that Reliability*First* accepted the Mitigation Plan on September 26, 2008.

EXPECTED COMPLETION DATE **10/31/08**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **9/30/08**

DATE OF CERTIFICATION LETTER **10/21/08**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **9/30/08**

DATE OF VERIFICATION LETTER **6/11/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **9/30/08**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE completed the following actions:**

- **The quarterly, software generated preventive maintenance order in URE's system for battery maintenance at a facility was adjusted so the work order is triggered two weeks prior to the beginning of each quarter;**
- **All work orders for NERC-required maintenance activities were modified to include in the title "NERC Required" to emphasize the importance of scheduling and completing the orders;**
- **A quarterly auto notification in Microsoft Outlook was set up to confirm completion of quarterly battery maintenance by the plant Electrical Engineer; and**
- **Additional training was conducted to emphasize the importance of timely maintenance and testing.**

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

- **A document that lists the two battery testing work orders generated from the maintenance management system but not scheduled in the second quarter of 2008.**
- **A document that identifies the batteries for one of its plants.**
- **A document that verifies that the Unit 2 station batteries consist of 1 set of 60 cells.**
- **A document that identifies the batteries for Unit 3.**
- **A document verifies that the Unit 3 station batteries consist of 1 set of 60 cells.**
- **URE Letter to Reliability*First* in response to a Request for Information.**
- **In addition, a review of six work orders verified that the 2008 third and fourth quarter battery testing as well as the 2009 first quarter battery testing was completed within the proper quarter.**

EXHIBITS:

SOURCE DOCUMENT
**Self-Report dated September 16, 2008**

**Self-Certification dated September 23, 2008**

MITIGATION PLAN
**Mitigation Plan dated September 17, 2008**

CERTIFICATION BY REGISTERED ENTITY
**Certification of Mitigation Plan Completion dated October 21, 2008**

VERIFICATION BY REGIONAL ENTITY
**Verification of Mitigation Plan Completion dated June 11, 2010**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-004-1 R4, R2, R3, R3 and R4.1

# DISPOSITION OF VIOLATION
## Dated September 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC200900125** | **RFC200900125** |
| **RFC200900135** | **RFC200900135** |
| **RFC200900136** | **RFC200900136** |
| **RFC200900197** | **RFC200900197** |
| **RFC200900198** | **RFC200900198** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-004-1** | **4** | **4.1, 4.2** | **Medium**[1] | **High** |
| **CIP-004-1** | **2** | **2.1, 2.3** | **Medium**[2] | **Lower** |
| **CIP-004-1** | **3** | **3.1, 3.3** | **Medium**[3] | **Moderate** |
| **CIP-004-1** | **3** | | **Medium**[4] | **Moderate** |
| **CIP-004-1** | **4** | **4.1** | **Lower** | **Lower** |

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

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

[1] When NERC filed Violation Risk Factors (VRFs), it originally assigned CIP-004-1 R4.2 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R4.2 was in effect from June 18, 2007 until January 27, 2009 when the "Medium" VRF became effective. CIP-004-1 R4 and R4.1 have "Lower" VRFs.

[2] When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

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

[4] *Id*.

**CIP-004-1 R2, R3 and R4 provide in pertinent part:**

**R2. Training — The Responsible Entity[5] 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.**

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

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

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

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

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

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

**R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:**

**R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing**

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

**collective bargaining unit agreements, depending upon the criticality of the position.**

**R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.**

**R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.**

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

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

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

VIOLATION DESCRIPTION

**URE submitted three Self-Reports related to access to Critical Cyber Assets and Personnel Risk Assessments (PRAs). The first was originally submitted on February 27, 2009. A second self-report was submitted on April 24, 2009, which amended the violation reported on February 27, 2009 and reported two additional violations. These self-reports resulted in violations RFC200900125, RFC 200900135, and RFC200900136. The third Self-Report was submitted on September 16, 2009 and resulted in violations RFC200900197 and RFC200900198.**

**<u>February 27, 2009 and April 24, 2009 Self-Reports</u>**

***CIP-004-1 R4 – RFC200900125***
**During a routine review of its compliance documentation on February 13, 2009, URE discovered that six employees included on the list of personnel with access to System Operations (SO) and back-up SO areas did not have PRAs completed. URE revoked unescorted physical access rights for these employees on February 13, 2009**

**and initiated an internal investigation. As part of the investigation, URE conducted a review of both the SO access list and the PRA list to determine whether both lists were complete.**

**On February 20, 2009, URE found during a root cause analysis that six employees (discussed above) and four contract workers had unescorted physical access to URE's SO and back-up SO areas after the effective date of CIP-004-1 without having PRAs.[6] URE revoked unescorted physical access rights for the contract workers on February 24, 2009. After revoking the unescorted physical access rights for the six employees and four contract workers, URE completed PRAs for the two employees who had entered the SO area and the four contract workers who accessed the back-up SO area; no issues with any personnel were identified in the referenced PRAs.**

**On February 27, 2009, URE self-reported the violation indicating a violation of CIP-004-1 R4.2[7] because URE determined that the six employees did not require access and therefore, URE failed to revoke access within seven calendar days for personnel who did not require access.**

**After submitting the Self-Report and following two informal discussions with Reliability*First*, URE conducted a comprehensive follow-up review to determine whether any additional areas of non-compliance existed with respect to any of the CIP Standards. On April 24, 2009, URE submitted an amended Self-Report and a Supplemental Narrative document which amended the originally self-reported violation of R4 and reported violations of CIP-004-1 R2, specifically R2.1 and R2.3, and CIP-004-1 R3, specifically R3.1 and R3.3 (discussed below).**

**In the amended Self-Report and Supplemental Narrative, URE reported that it also determined that its access lists of personnel with authorized cyber and unescorted physical access to Critical Cyber Assets were incomplete. URE did not maintain a complete list of all personnel with access. As a result, URE reviewed an incomplete access list in the third quarter 2008, which did not include personnel with cyber access or contractors and service providers with physical access, to Critical Cyber Assets. In addition, URE did not conduct a fourth quarter 2008 review of its access list. Finally, URE completed the first quarter 2009 review in a timely fashion; however, it did not list access to specific Critical Cyber Assets.**

***CIP-004-1 R2 – RFC200900135***
**As detailed in the April 24, 2009 Self-Report, URE reported non-compliance with CIP-004-1, R2.1 and R2.3, for failing to ensure that all personnel with access to**

[6] Two of the six employees entered the SO after the effective date of CIP-004-1, but both were under escort, attending meetings, when they did so. The other four employees never attempted to enter the SO after the effective date of CIP-004-1. The four contract workers were long-term contract workers who accessed the back-up SO area to perform routine janitorial work before and after the effective date of CIP-004-1.

[7] Page 3 of the Self-Report incorrectly states non-compliance with CIP-004-1 R2.1.6 and incorrectly states that three contract workers, instead of four, retained unescorted access.

**Critical Cyber Assets were trained within 90 days of such access. URE improperly granted 47 out of 83 total URE employees the right to cyber access or authorized unescorted physical access to Critical Cyber Assets, who did not attend annual training within 90 calendar days of receiving such authorization.**

**URE maintained training attendance records for some employees, but could not provide training records for all employees, contractors, and service providers with physical or cyber access rights to the SO and back-up SO areas. Although some of the employees for whom training records did not exist asserted that they received training, URE determined that if it did not have training records for an employee, that employee was not trained.**

**Upon discovering the lack of training records, URE revoked access for those employees, contractors and service providers for whom there were no training records.**

***CIP-004-1 R3 – RFC200900136***
**In April 24, 2009 Self Report, URE reported non-compliance with CIP-004-1 R3.1 and R3.3 for failing to conduct timely PRAs on 21[8] of its 83 employees, contractors and service providers who had unescorted physical and/or cyber access rights to a Critical Cyber Asset.[9]**

**URE revoked access rights for the employees, contractors, and service providers for whom there was no PRA as soon as the documentation issues were identified. URE completed PRAs for all employees (except one who was out of the office due to long-term illness[10]), contractors, and service providers who both (a) remained employed or contracted with URE; and (b) needed physical or cyber access rights to Critical Cyber Assets.**

**September 16, 2009 Self-Report**

***CIP-004-1 R3 – RFC200900197[11]***
**On September 16, 2009, URE submitted a separate Self-Report regarding a second violation of CIP-004-1 R3 for failing to complete a PRA within thirty (30) days for a contract worker that was inadvertently granted access to the SO area. Through an**

[8] URE discovered this violation with respect to 10 of the personnel in February 2009 which was included in the February 27, 2009 self-reported violation of CIP-004-1 R4.2. The additional 11 personnel were discovered as a result of the comprehensive follow-up investigation performed by URE.
[9] URE conservatively interpreted "unescorted access" to mean access by a person that was not continuously in the line of sight of URE personnel. Persons entering SO always were signed in at the secured entry point by URE personnel. However, some personnel worked on equipment located in a separate room inside SO, and at times these persons were "unescorted" because they were not in the line of sight of URE personnel.
[10] At the time the Settlement Agreement was executed, this employee was still out of the office. This employee subsequently returned, and URE completed a PRA for the employee immediately upon her return.
[11] For purposes of penalty determination, Reliability*First* considered URE's second violation of CIP-004-1, R3 (RFC200900197) and of CIP-004-1 R4 (RFC200900198) to be an aggravating factor because the violations were not related to a single act or common incidence of non-compliance.

**investigation into the cause of the violation, URE determined that a lack of functionality in the legacy access control system permitted the inadvertent grant of access.**

**URE granted the contract worker access to the SO area on July 13, 2009. URE was required to complete a PRA on the contract worker by August 12, 2009, thirty (30) days after URE granted the access. Instead, URE only revoked the contract worker's access upon discovering the inadvertent grant of access on September 3, 2009, 22 days after the expiration of the 30-day period.**

***CIP-004-1 R4/4.1 – RFC200900198***
**The September 16, 2009 Self-Report also included a second violation of CIP-004-1 R4.1 for failing to update its master list of personnel with authorized cyber or unescorted physical access rights to a Critical Cyber Asset within seven days of granting that access. As discussed above, URE discovered that it inadvertently gave a contract worker an access card on July 13, 2009, granting him the right to unescorted access to the SO area. This resulted in URE's failure to update its master list of personnel with authorized cyber or unescorted physical access rights to a Critical Cyber Asset within seven days of granting that access, as required by R4.1.**

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

**Reliability*First* determined that the first violation of CIP-004-1 R4 (RFC200900125) did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because four of the six employees with unescorted physical access rights, never attempted to enter the SO. The two employees that entered the SO were attending meetings and were escorted at all times by URE employees with authorized access and completed PRAs. The four contract workers were long-term contract workers who accessed the back-up SO area to perform routine janitorial work. Additionally, after revoking unescorted access for the ten employees and contract workers, URE completed PRAs for the two employees who had entered the SO area and the four contract workers who accessed the backup SO area and identified no issues.**

**Reliability*First* determined that the violation of CIP-004-1 R2 (RFC200900135) did not pose a serious or substantial risk to the reliability of the BPS because some of the employees for which training records are not available asserted that they have received training, and URE has now completed and documented training for all employees, contractors and service providers who remain employed or engaged at URE and have physical or cyber access to Critical Cyber Assets.**

**Reliability*First* determined that the first violation of CIP-004-1 R3 (RFC200900136) did not pose a serious or substantial risk to the reliability of the BPS because people that entered the SO area were always signed in at a secured entry point by URE personnel and therefore, there was at least some accountability on the part of the**

**employees who may exercise their access rights as well as a mechanism to trace back any access in the event that access was improperly exercised. Additionally, URE has now completed PRAs for all employees (with the exception of one who has been out of the office with a long term illness), contractors and providers who remain employed or engaged at URE and who currently have physical or cyber access to Critical Cyber Assets.**

**Reliability*First* determined that the second violations of CIP-004-1 R3 (RFC200900197) and CIP-004-1 R4/4.1 (RFC200900198) under the September 16, 2009 Self-Report did not pose a serious or substantial risk to the reliability of the BPS because URE verified that the contract employee had not accessed the SO area during the time his badge enabled him to do so and that he was not aware that he had access rights to the SO. URE reviewed the log of the employee's card to determine that the card was not used to gain access to Critical Cyber Assets. Also, URE interviewed the contract employee, determined the contract employee's understanding of his access rights, and verified that the contract employee had not attempted or gained access to any Critical Cyber Assets.**

## II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S)

**CIP-004-1 R4 (RFC200900125): 7/1/08 (when the Standard became mandatory and enforceable for Table 1 entities with Critical Cyber Assets at its System Control Center) through 7/1/09 (when URE mitigated the violation)**

**CIP-004-1 R2 (RFC200900135): 7/1/08 (when the Standard became mandatory and enforceable for Table 1 entities with Critical Cyber Assets at its System Control Center) through 7/1/09 (when URE mitigated the violation)**

**CIP-004-1 R3 (RFC200900136): 7/1/08 (when the Standard became mandatory and enforceable for Table 1 entities with Critical Cyber Assets at its System Control Center) through 7/1/09 (when URE mitigated the violation)**

**CIP-004-1 R3 (RFC200900197): 8/13/09 (the date URE failed to complete a PRA within 30 days) through 10/1/09 (when URE mitigated the violation)**

**CIP-004-1 R4.1 (RFC200900198): 7/21/09 (the date URE failed to update its master list) through 10/1/09 (when URE mitigated the violation)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **2/27/09, 4/24/09 and 9/16/09**

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

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

## III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:
MITIGATION PLAN NO. **MIT-08-2311**[12]
DATE SUBMITTED TO REGIONAL ENTITY **1/20/10**[13]
DATE ACCEPTED BY REGIONAL ENTITY **2/1/10**
DATE APPROVED BY NERC **2/9/10**
DATE PROVIDED TO FERC **2/9/10**

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 **11/10/09**
DATE OF CERTIFICATION LETTER **2/12/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **11/10/09**

DATE OF VERIFICATION LETTER **4/5/10**[14]
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **11/10/09**

[12] *See* n.1 though n.4 *supra* to explain the VRFs in the Mitigation Plan.
[13] The Narrative Supplement submitted by URE with its April 24, 2009 self-report states that URE had submitted a Mitigation Plan for RFC200900125 and subsequently withdrew it. Reliability*First* considered the initial Mitigation Plan to be a draft.
[14] The Settlement Agreement incorrectly states that the document is dated April 25, 2010.

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE revoked all improper access rights, developed a comprehensive list of all employees, contractors, and service providers with access to Critical Cyber Assets, and developed a process to keep the access list updated. URE completed all necessary cyber security training and PRAs, and developed a process to keep training and PRAs updated. URE implemented a procedure that requires URE's corporate security specialist and the manager of corporate security to review each access change that involves Critical Cyber Assets. URE created a cyber security working group to review and provide continuing feedback on CIP procedures, policies, and practices at URE.**

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)

**To verify mitigation of the violations of CIP-004-1 R2, R3 and R4, Reliability*First* reviewed several attachments to URE's *Amended Narrative Supplement to ReliabilityFirst Violation Self Reporting Form* dated April 24, 2009.**

**Reliability*First* also reviewed the following:**

- **For R2: an e-mail dated November 19, 2009 describing URE's Web-based tracking system for training which included the date training was completed and the date the next training is required.**
- **For R3: a document describing URE's new procedure requiring the corporate security specialist and his supervisor, the manager of corporate security, to review each access change that involves Critical Cyber Assets.**
- **For R4: an example of the new access list developed with URE's new internal processes for updating its list.**

EXHIBITS:

SOURCE DOCUMENT
**Self-Report for CIP-004-1 R4 (RFC200900125) dated February 27, 2009**

**Self-Report for CIP-004-1 R4 (RFC200900125), CIP-004-1 R2 (RFC200900135) and CIP-004-1 R3 (RFC200900136) dated April 24, 2009**

**Narrative Supplement to Reliability*First* Violation Self Reporting Form for CIP-004-1 R4 (RFC200900125), CIP-004-1 R2 (RFC200900135) and CIP-004-1 R3 (RFC200900136) dated April 24, 2009**

**Self-Report for CIP-004-1 R3 (RFC200900197) and CIP-004-1 R4.1 (RFC200900198) dated September 16, 2009**

MITIGATION PLAN
**Mitigation Plan dated January 20, 2010**

CERTIFICATION BY REGISTERED ENTITY
**Certification of Mitigation Plan Completion dated February 12, 2010**

VERIFICATION BY REGIONAL ENTITY
**Verification of Mitigation Plan Completion dated April 5, 2010**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-007-1 R1

# DISPOSITION OF VIOLATION
## Dated September 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC200900137** | **RFC200900137** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-007-1** | **1** | **1.1** | **Medium** [1] | **High** |

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[2] 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 CIP007 should be read as part of a group of standards numbered Standards CIP-002 though CIP-009…" (Footnote added)**

**CIP-007-1 R1 provides in pertinent part:**

> **R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.**
>
> > **R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.**

[1] CIP-007-1 R1 and R1.1 each have a Medium Violation Risk Factor (VRF); R1.2 and R1.3 each have a Lower VRF.

[2] 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.

VIOLATION DESCRIPTION

**On April 24, 2009, URE self-reported a violation of CIP-007-1 R1 for failure to document its cyber security test procedures, which are required to minimize the adverse effect of new Cyber Assets and significant changes to existing Cyber Assets on the production system and its operation.**

**Upon investigation, URE evaluated the new Cyber Assets it had implemented without a documented test procedure. URE determined that new, replacement firewalls were configured and placed into production on February 23, 2009 with a redundant system available for recovery, and that one new Cyber Asset was placed into production on March 9, 2009. No other significant changes to existing Cyber Assets occurred since the effective date of CIP-007-1 R1.**

**URE documented the testing and completion of the firewall configuration and installation on February 23, 2009, the same day it was installed. URE completed testing of the new Cyber Asset on March 9, 2009, the same day it was placed into production, and approved documentation of the testing on March 11, 2009. URE performed additional actions to strengthen the firewalls between March 26, 2009 and March 31, 2009.**

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 because URE tested new Cyber Assets within its electronic security perimeter, since the effective date of the Standard. While URE did not have a documented cyber security test procedure in place; URE tested and documented the configuration of the referenced two new Cyber Assets placed into production on the same day those Cyber Assets were installed.**

## II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) **7/1/08 (when the Standard became mandatory and enforceable for Table 1 entities with Critical Cyber Assets at its System Control Center) through 4/27/09 (Mitigation Plan completion)**
DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **4/24/09**

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

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

## III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:
MITIGATION PLAN NO. **MIT-08-1985**
DATE SUBMITTED TO REGIONAL ENTITY **9/4/09**
DATE ACCEPTED BY REGIONAL ENTITY **9/14/09**[3]
DATE APPROVED BY NERC **9/23/09**
DATE PROVIDED TO FERC **9/23/09**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **4/27/09**

DATE OF CERTIFICATION LETTER **9/28/09 (submitted 9/29/09)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **4/27/09**

DATE OF VERIFICATION LETTER **10/27/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **4/27/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
**URE developed cyber security test procedures. URE then implemented the cyber security test procedures, and completed training on the cyber security test procedures.**

[3] Reliability*First*'s Verification of Completion incorrectly states that Reliability*First* accepted URE's Mitigation Plan on September 18, 2009.

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)

**Reliability*First* reviewed the following documents:**

- **CIP-007 R1 Security test procedures; and**
- **Document attesting that all URE Supervisory Control and Data Acquisition (SCADA) maintenance personnel in the Systems Operations department were trained on the new security test procedures on April 27, 2009.**

EXHIBITS:

SOURCE DOCUMENT
**Self-Report dated April 24, 2009**

**Narrative Supplement to Reliability*First* Violation Self Reporting Form dated April 24, 2009**

MITIGATION PLAN
**Mitigation Plan dated September 4, 2009**

CERTIFICATION BY REGISTERED ENTITY
**Certification of Mitigation Plan Completion dated September 28, 2009**

VERIFICATION BY REGIONAL ENTITY
**Verification of Mitigation Plan Completion dated October 27, 2009**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-008-1 R1

# DISPOSITION OF VIOLATION
## Dated September 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC200900138** | **RFC200900138** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-008-1** | **1** | **1.4, 1.5, 1.6** | **Lower** | **High**[1] |

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

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

**CIP-008-1 R1 provides in pertinent part:**

> **R1. Cyber Security Incident Response Plan — The Responsible Entity[2] shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:**
>
> **…**
>
> **R1.4. Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.**
>
> **R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.**
>
> **R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.**

**(Footnote added.)**

[1] The Self-Report incorrectly states that the VSL is Moderate.
[2] Within the text of Standard CIP-008, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

VIOLATION DESCRIPTION

**URE self-reported a violation of CIP-008-1 R1 on April 24, 2009 for maintaining a Cyber Security Incident response plan (Plan) that did not include URE's processes for (a) updating the Plan within ninety calendar days of any changes as required by CIP-008-1 R1.4; (b) conducting annual reviews of the Plan as required by CIP-008-1 R1.5; or (c) testing the Plan on an annual basis as required by CIP-008-1 R1.6.**

**URE's Plan did include procedures to characterize and classify events as reportable Cyber Security Incidents, response actions, incident handling procedures and communications plans as required by R1.1 and R1.2. URE's Plan also included a process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center as required by R1.3.**

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 because, while there were no detailed processes regarding updating, reviewing, or testing URE's Plan, the Plan did state that URE would update the procedures within ninety days of any changes, conduct annual reviews of the Plan and test the Plan on an annual basis. Further, URE followed its Plan as written.**

## II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) **7/1/08 (when the Standard became mandatory and enforceable for Table 1 entities with Critical Cyber Assets in its System Control Center) through 4/24/09 (Mitigation Plan completion)**

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

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

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

## III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **MIT-08-1986**
DATE SUBMITTED TO REGIONAL ENTITY **9/4/09**
DATE ACCEPTED BY REGIONAL ENTITY **9/14/09**[3]
DATE APPROVED BY NERC **9/23/09**
DATE PROVIDED TO FERC **9/23/09**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **Submitted as complete**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **4/24/09**

DATE OF CERTIFICATION LETTER **9/28/09 (submitted 9/29/09)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **4/24/09**

DATE OF VERIFICATION LETTER **10/7/09**[4]
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **4/24/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE revised its Plan to include procedures to (a) update the Plan within ninety calendar days of any changes affecting the Plan; (b) ensure the Plan is reviewed at least annually; and (c) ensure the Plan is tested on an annual basis. URE then implemented its revised Plan.**

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)

**Reliability*First* reviewed the following documents:**

- **URE's revised Cyber Security Incident response plan**

[3] Reliability*First*'s Verification of Completion incorrectly states that Reliability*First* accepted the Mitigation Plan on September 18, 2009.
[4] The Verification of Completion is incorrectly dated October 15, 2009 on the front page.

EXHIBITS:

SOURCE DOCUMENT
**Self-Report dated April 24, 2009**

**Narrative Supplement to Reliability*First* Violation Self Reporting Form dated April 24, 2009**

MITIGATION PLAN
**Mitigation Plan dated September 4, 2009**

CERTIFICATION BY REGISTERED ENTITY
**Certification of Mitigation Plan Completion dated September 28, 2009**

VERIFICATION BY REGIONAL ENTITY
**Verification of Mitigation Plan Completion dated October 7, 2009**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for EOP-001-0 R6

# DISPOSITION OF VIOLATION
## Dated September 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC200900148** | **RFC200900148** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **EOP-001-0** | **6** | | **Medium** | **Severe** |

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

**The purpose statement of EOP-001-0 provides: "Each Transmission Operator and Balancing Authority needs to develop, maintain, and implement a set of plans to mitigate operating emergencies. These plans need to be coordinated with other Transmission Operators and Balancing Authorities, and the Reliability Coordinator."**

**EOP-001-0 R6 provides: "The Transmission Operator and Balancing Authority shall annually review and update each emergency plan. The Transmission Operator and Balancing Authority shall provide a copy of its updated emergency plans to its Reliability Coordinator and to neighboring Transmission Operators and Balancing Authorities."**

VIOLATION DESCRIPTION

**In preparation for an upcoming audit conducted, URE self-reported a violation of EOP-001-0 R6 on May 14, 2009[1] for failing to provide copies of its updated emergency plans to its neighboring Transmission Operators (TOP)[2] and Balancing Authorities (BA) in 2007. In 2007, URE and its neighboring TOPs participated in a series of emergency planning drills led by their Reliability Coordinator (RC). During the course of the drills, the participants (including URE) reviewed their emergency plans with one another.**

**Although URE had a copy of the RC's agenda for the drill, evidence of its participation in the drill and evidence that it provided emergency plans to the RC in 2007, URE could not document that it provided physical copies of its emergency plans to its neighboring TOPs and BAs in 2007. URE did have evidence that it**

[1] Reliability*First*'s Verification of Completion incorrectly states that URE self-reported this violation on April 24, 2009.
[2] The Settlement Agreement and Mitigation Plan incorrectly refer to Transmission Owners instead of Transmission Operators.

**provided its emergency plans to its neighboring TOPs, neighboring BAs, and RC in 2008.**

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 because, while URE did not formally provide copies of its 2007 emergency plans to neighboring BAs and TOPs, it did review them with the neighboring BAs and TOPs during the drills led by the RC, and it provided the emergency plans to the RC.**

## II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

| | |
|---|---|
| SELF-REPORT | ☒[3] |
| SELF-CERTIFICATION | ☐ |
| COMPLIANCE AUDIT | ☐ |
| COMPLIANCE VIOLATION INVESTIGATION | ☐ |
| SPOT CHECK | ☐ |
| COMPLAINT | ☐ |
| PERIODIC DATA SUBMITTAL | ☐ |
| EXCEPTION REPORTING | ☐ |

DURATION DATE(S) **6/18/07 (when the Standard became mandatory and enforceable) through 8/4/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **5/14/09**

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

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

## III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

| | |
|---|---|
| MITIGATION PLAN NO. | **MIT-09-2050** |
| DATE SUBMITTED TO REGIONAL ENTITY | **9/28/09** |
| DATE ACCEPTED BY REGIONAL ENTITY | **10/9/09** |
| DATE APPROVED BY NERC | **10/20/09** |
| DATE PROVIDED TO FERC | **10/20/09** |

[3] Although URE submitted a self-report for this violation, it was submitted in preparation for an upcoming Audit.

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 **8/4/09**

DATE OF CERTIFICATION LETTER **11/20/09 (signed 11/19/09)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **8/4/09**

DATE OF VERIFICATION LETTER **12/2/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **8/4/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE documented and formalized its procedure governing the sharing of its emergency plans with its neighboring BAs and TOPs. URE then implemented its procedure.**

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)

**Reliability*First* reviewed the following evidence:**

- **Emergency plans coordination procedure; and**
- **Copies of e-mails dated August 2009 showing that URE provided copies of its emergency plans in 2008 with its RC and neighboring BAs and TOPs.**

EXHIBITS:

SOURCE DOCUMENT
**Self-Report dated May 14, 2009**

MITIGATION PLAN
**Mitigation Plan dated September 28, 2009**

CERTIFICATION BY REGISTERED ENTITY
**Certification of Mitigation Plan Completion submitted November 20, 2009**

VERIFICATION BY REGIONAL ENTITY
**Verification of Mitigation Plan Completion dated December 2, 2009**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for PRC-005-1 R1

# DISPOSITION OF VIOLATION
## Dated September 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC200900149** | **RFC200900149** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **PRC-005-1** | **1** | | **High**[1] | **Lower** |

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

**The purpose statement of PRC-005-1 provides: "To ensure all transmission and generation Protection Systems[2] affecting the reliability of the Bulk Electric System (BES) are maintained and tested." (Footnote added)**

**PRC-005-1 R1 provides:**

> **R1. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES." The program shall include:**
>
> > **R1.1. Maintenance and testing intervals and their basis.**
> >
> > **R1.2. Summary of maintenance and testing procedures.**

VIOLATION DESCRIPTION

**On April 24, 2009, URE self-reported a violation of PRC-005-1 R1 because, prior to December 3, 2007, URE failed to have a complete maintenance and testing program in place for its generation Protection System as required by PRC-005-1 R1.**

---

[1] When NERC filed Violation Risk Factors (VRF) it originally assigned PRC-005-1 R1 a Medium VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on August 9, 2007, the Commission approved the modified High VRF. Therefore, the Medium VRF for PRC-005-1 R1 was in effect from June 18, 2007 until August 9, 2007 when the High VRF became effective.

[2] *The NERC Glossary of Terms Used in Reliability Standards* defines Protection System as "Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry."

**During an on-site audit of URE, the Reliability*First* audit team (Audit Team) reviewed URE's generation Protection System Maintenance and Testing plan and procedures. The Audit Team determined that although the procedures covered URE's generation Protection System, URE's Protection System maintenance and testing program (Program) did not have basis for the maintenance and testing interval or a summary of maintenance and testing procedures for (7.8%) DC control circuitry devices on five generators: Unit #1, Unit #2, Unit #3, and Unit #4 at one plant, and Unit #3 at a second plant. URE did, however, monitor and perform DC ground mitigation on the referenced DC control circuitry devices.**

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 because, even though DC control circuitry devices were not included in the formal maintenance and testing program, URE monitored and performed DC ground mitigation on the referenced DC control circuitry devices. URE indicated that based upon third quarter 2009 maintenance and testing, all DC control circuitry devices were operating properly.**

## 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) **6/18/07 (when the Standard became mandatory and enforceable) through 8/26/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

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-07-2562**
DATE SUBMITTED TO REGIONAL ENTITY **6/10/10**
DATE ACCEPTED BY REGIONAL ENTITY **6/18/10**
DATE APPROVED BY NERC **6/30/10**
DATE PROVIDED TO FERC **6/30/10**

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 **8/26/09**

DATE OF CERTIFICATION LETTER **6/22/10 (signed 6/21/10)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **8/26/09**

DATE OF VERIFICATION LETTER **8/20/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **8/26/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE completed the maintenance and testing procedures for its Program. URE revised its Program to include maintenance and testing intervals and their basis, and maintenance and testing procedures for DC control circuitry. URE completed maintenance and testing on the devices URE added to its Program.**

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 assembled a team to develop a generation Protection System Maintenance and Testing Plan needed to achieve PRC-005-1 compliance. Reliability*First* verified this action as complete by reviewing the document and training records, which included the names and signatures of the personnel in attendance.**

**URE completed and implemented its generation Protection System Maintenance and Testing Plan. Reliability*First* verified this action as complete by**

**reviewing the generation Protection System Maintenance and Testing Plan, effective December 3, 2007. This action was intended to bring URE's generation Protection Systems maintenance and testing program into compliance with PRC-005-1, Requirement 1. However, an audit by Reliability*First* determined that URE's generation maintenance and testing program was still deficient and required additional enhancements.**

**URE convened a work group to identify and implement mitigation measures addressing the PRC-005-l possible alleged violation that Reliability*First* identified during the Audit. Reliability*First* verified this action as complete by reviewing the post audit meeting attendance list, with periodic updates. These documents indicate the dates and attendance of work group meetings and identify the accountable persons assigned to specific tasks as well as the progress of those tasks.**

**URE revised its generation Protection System maintenance and testing procedures to include (1) maintenance and testing intervals and their basis and (2) maintenance and testing procedures for DC control circuitry. URE combined and standardized its transmission Protection System maintenance and testing plan and its generation Protection System maintenance and testing plan procedures into a single procedure.**

**Reliability*First* verified these mitigating actions as complete by reviewing the transmission and generation Protection System Maintenance and Testing Plan, effective June 19, 2009. These action brought URE's generation Protection Systems maintenance and testing program into compliance with PRC-005-1, Requirement 1. In addition, the combined document eliminated possible confusion caused by different procedures, thereby increasing the likelihood of future compliance with PRC-005-1.**

**URE completed maintenance and testing on generation DC control circuitry using the revised procedures. Reliability*First* verified these actions as complete by reviewing Preventative Maintenance Work Orders dated July 16, 2009 through August 26, 2009. These indicate that the DC Control Circuitry added to URE's revised procedures was maintained and tested in accordance with those procedures.**

EXHIBITS:

SOURCE DOCUMENT
**Self-Report dated April 24, 2009**

**Narrative Supplement to Reliability*First* Violation Self Reporting Form dated April 24, 2009**

MITIGATION PLAN
**Mitigation Plan dated June 10, 2010**

CERTIFICATION BY REGISTERED ENTITY
**Certification of Mitigation Plan Completion dated June 22, 2010**

VERIFICATION BY REGIONAL ENTITY
**Verification of Mitigation Plan Completion dated August 20, 2010**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for FAC-009-1 R1

# DISPOSITION OF VIOLATION
## Dated September 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC200900150** | **RFC200900150** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **FAC-009-1** | **1** | | **Medium** | **Moderate** |

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

**The purpose statement of FAC-009-1 provides: "To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies."**

**FAC-009-1 R1 provides: "The Transmission Owner and Generator Owner shall each establish Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology."**

VIOLATION DESCRIPTION

**During an on-site compliance audit conducted by Reliability*First*, the Reliability*First* audit team (Audit Team) determined that URE failed to establish Facility Ratings that were consistent with its Facility Ratings Methodology. The Audit Team examined the URE Facility Ratings Methodology (Methodology) and found that the ratings URE provided for one of its plant's Unit #3 facility were inconsistent and did not demonstrate that URE established Facility Ratings for its solely and jointly owned facilities that were consistent with its Methodology.**

**The Audit Team also found that the Facility Rating Table (Table) for a second plant's facilities did not have ratings for the generator step-up transformer low voltage current transformers. The Table indicated that no nameplate rating was given by the manufacturer for this equipment, in contrast with the Methodology's statement that current transformers are rated at the manufacturer's nameplate continuous rating for both normal and emergency ratings.**
**The Table showed generator nameplate ratings and not the net MW ratings. The Table did not provide the limits for all elements in consistent units (*e.g.*, amperes or megavolt amperes), and in some cases showed that other elements comprising the facility may be more limiting than the generator nameplate rating.**

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 because Power Flow studies of the URE system demonstrated that a Category B or Category C contingency event that might result from an incorrect Facility Rating creates no overloads or voltage problems that URE could not quickly correct by switching, redispatching generation, or shedding local load. Further, the Power Flow studies demonstrated that a Category D extreme contingency will not affect the bulk electric system because such a contingency event would not result in cascading effects beyond the URE ties and onto the Bulk Power System, even if URE were to lose its entire system. Additionally, when URE revised its Facility Ratings, URE determined that both the revised ratings and the original ratings reflected the most limiting element.**

## 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) **6/18/07 (when the Standard became mandatory and enforceable) through 8/24/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

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-07-2551**
DATE SUBMITTED TO REGIONAL ENTITY **5/21/10**
DATE ACCEPTED BY REGIONAL ENTITY **5/26/10**
DATE APPROVED BY NERC **6/25/10**
DATE PROVIDED TO FERC **6/28/10**

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 **8/24/09**

DATE OF CERTIFICATION LETTER **6/2/10 (signed 5/28/10)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **8/24/09**

DATE OF VERIFICATION LETTER **7/14/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **8/24/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE reviewed all the equipment in the electrical path from the generator to the switchyard for each unit. URE converted all ratings to a common unit of measure (amperes) and identified the most limiting element for each unit. URE revised its Methodology to establish Facility Ratings using nameplate data, where available, and manufacturers recommendations where nameplate data is not available. URE implemented its revised Methodology.**

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 transmission and generation System Facility Rating's Methodology document.**
- **A letter that provides clarification of the ratings of components associated with the GE power transformers at two of URE's stations.**
- **Generator Step-Up Main Transformer nameplate data.**
- **Equipment ratings and GSU labels at two of its facilities which verified that URE is using Generator nameplate data.**

**EXHIBITS:**

**SOURCE DOCUMENT**
**Reliability*First*'s Public Audit Report**

**MITIGATION PLAN**
**Mitigation Plan dated May 21, 2010**

CERTIFICATION BY REGISTERED ENTITY
**Certification of Mitigation Plan Completion submitted June 2, 2010**

VERIFICATION BY REGIONAL ENTITY
**Verification of Mitigation Plan Completion dated July 14, 2010**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for FAC-014-1 R2 and R4

# DISPOSITION OF VIOLATION
## Dated September 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC200900151** | **RFC200900151** |
| **RFC200900152** | **RFC200900152** |

## I. VIOLATION INFORMATION[1]

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **FAC-014-1[2]** | **2** | | **Medium** | **High** |
| **FAC-014-1[3]** | **4** | | **Medium** | **High** |

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

**The purpose statement of FAC-014-1 provides: "To ensure that System Operating Limits (SOLs) used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies."**

**FAC-014-1 R2 provides: "The Transmission Operator shall establish SOLs (as directed by its Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology."**

**FAC-014-1 R4 provides: "The Transmission Planner shall establish SOLs, including IROLs, for its Transmission Planning Area that are consistent with its Planning Authority's SOL Methodology."**

VIOLATION DESCRIPTION

***FAC-014-1 R2***
**During an on-site audit of URE, the Reliability*First* audit team (Audit Team) determined that URE failed to establish SOLs, as directed by its Reliability Coordinator, that were consistent with its Reliability Coordinator's SOL Methodology. The Reliability Coordinator's Methodology for Identification and Implementation of Interconnection Reliability Operating Limits (IROLs) and**

[1] Based on the NERC Sanction Guidelines, Reliability*First* determined the violations of FAC-014-1 R2 and R4 were "related to a single act or common incidence of non-compliance" for which Reliability*First* would assess "a single aggregate penalty."
[2] FAC-014-1 was enforceable from January 1, 2009 through April 28, 2009. FAC-014-2 is the current enforceable Standard as of April 29, 2009.
[3] *Id*.

**SOLs' (SOL Methodology) requires URE to establish SOLs that are not greater than URE's Facility Ratings.**

**URE provided the Audit Team with evidence of the SOLs, however, the flowgate limits in these lists were not representative of all URE SOLs. In some cases, the SOLs provided to the Reliability Coordinator were greater than the Facility Ratings. The Audit Team found that 51% percent of URE's SOLs were inconsistent with the Reliability Coordinator's Methodology. Of these, 28% percent of URE's SOLs were greater than URE's Facility Ratings.**

***FAC-014-1 R4***
**The Audit Team also determined that URE failed to establish SOLs that were consistent with its Planning Authority's SOL Methodology. The Planning Authority SOL Methodology requires URE to establish SOLs that are not greater than URE's Facility Ratings.**

**URE provided the Audit Team with lists of its IROLs and SOLs, however, the flowgate limits in these lists were not representative of all URE IROLs and SOLs. Of the URE facilities that comprise URE's portion of the BPS 58% of the facilities had URE Facility Ratings inconsistent with the final facility study values. Of these, 10% had URE SOLs higher than the Facility Ratings.**

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 because the facilities primarily serve local load and do not have a significant participation factor to the system or energy transfers. All but one of the ratings discrepancies involves either current transformers (CTs) and CT ratios, or jumper ratings for bus conductors, with the majority of ratings discrepancies caused by CT ratios. Additionally, most of these CTs were on metering devices, and a failure would only limit reading the full scale and would not impact 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)

**R2: 1/1/09 (when the Standard became mandatory and enforceable) through 6/30/09 (Mitigation Plan completion)**[4]

**R4: 1/1/09 (when the Standard became mandatory and enforceable) through 8/24/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

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-09-2549**
DATE SUBMITTED TO REGIONAL ENTITY **5/21/10**
DATE ACCEPTED BY REGIONAL ENTITY **5/26/10**
DATE APPROVED BY NERC **6/15/10**
DATE PROVIDED TO FERC **6/15/10**

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 **8/24/09**

DATE OF CERTIFICATION LETTER **6/2/10 (signed 5/28/10)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **8/24/09**

DATE OF VERIFICATION LETTER **7/13/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **8/24/09**

[4] The Settlement Agreement incorrectly states that the start date of this violation is June 18, 2007.

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE identified the appropriate ratings for each facility, including the metering CTs, and determined whether URE's SOLs were consistent with those ratings. URE updated the facility ratings database to reflect the most limiting devices. URE submitted revised ratings to the Reliability Coordinator. URE revised its procedure implementing FAC-014-1 to be consistent with the Planning Authority's SOL Methodology and implemented its revised procedure.**

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)

**• Reliability Coordinator's Methodology for Identification, and Implementation of IROLs and SOLs.**
**• Planning Authority's SOL Methodology for the Planning Horizon,.**
**• URE*'s* generation and transmission System Facility Ratings.**
**• URE generation and transmission planning criteria.**
**• Ratings comparison table, undated.**
**• Submittal of Data to the Reliability Coordinator.**

EXHIBITS:

SOURCE DOCUMENT
**Reliability*First*'s Public Audit Report**

MITIGATION PLAN
**Mitigation Plan dated May 21, 2010**

CERTIFICATION BY REGISTERED ENTITY
**Certification of Mitigation Plan Completion dated June 2, 2010**

VERIFICATION BY REGIONAL ENTITY
**Verification of Mitigation Plan Completion dated July 13, 2010**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for TPL-002-0 R1

# DISPOSITION OF VIOLATION
## Dated September 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC200900153** | **RFC200900153** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **TPL-002-0** | **1** | **1.3, 1.3.1, 1.3.7** | **High**[1] | **Severe** |

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

**The purpose statement of TPL-002-0 provides: "System simulations and associated assessments are needed periodically to ensure that reliable systems are developed that meet specified performance requirements with sufficient lead time, and continue to be modified or upgraded as necessary to meet present and future system needs."**

**TPL-002-0 R1 provides in pertinent part:**

> **R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand levels over the range of forecast system demands, under the contingency conditions as defined in Category B of Table I. To be valid, the Planning Authority and Transmission Planner assessments shall:**
>
> **…**
>
> **R1.3. Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category B of Table 1 (single contingencies). The specific elements selected (from each of the following categories) for inclusion in these**

[1] TPL-002-1 R1 has a High Violation Risk Factor (VRF) and its sub-requirements have Medium VRFs. When NERC filed VRFs it originally assigned TPL-002-0 R1 a Medium VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on August 9, 2007, the Commission approved the modified High VRF. Therefore, the Medium VRF for TPL-002-0 R1 was in effect from June 18, 2007 until August 9, 2007 when the High VRF became effective.

**studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).**

**R1.3.1. Be performed and evaluated only for those Category B contingencies that would produce the more severe System results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.**

**…**

**R1.3.7. Demonstrate that system performance meets Category B contingencies.**

VIOLATION DESCRIPTION

**During an on-site audit of URE, the Reliability*First* audit team (Audit Team) determined that URE failed to demonstrate system performance was within limits (system stable) via dynamic studies or simulations for Category B contingencies. The Audit Team reviewed the dynamic study that URE conducted for the 2004 summer peak. The study included transient stability simulations of close-in Category D faults at two URE generating stations, and showed that the generators remained stable for close-in three phase faults with back-up clearance. URE did not simulate Category B contingencies in this study.**

**The Audit Team reviewed a 2007 report, which states that the dynamic study is used to evaluate the dynamic stability of the Reliability Coordinator's system in the summer of 2013 under various disturbances. The report also stated that the system was analyzed with the system intact as well as with 50 Category B, 139 Category C, and 79 Category D disturbances provided by Transmission Owners or selected from previous studies. No URE Category B contingencies were analyzed in this report. URE was not able to provide the rationale for the Category B contingencies selected for evaluation or an explanation of why the remaining simulations would produce less severe system results.**

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

**Reliability*First* determined that this violation did not pose a serious or substantial risk to the bulk power system because, although URE did not perform Category B or Category C contingency studies, URE did perform Category D contingency studies. Power Flow studies of the URE South system demonstrate that a Category B or Category C contingency event that might result from an incorrect Facility Rating creates no overloads or voltage problems that URE could not quickly correct by switching, redispatching generation, or shedding local load. Further, the Power**

**Flow studies demonstrate that the Category D extreme contingencies studied would not result in instability leading to a cascade. Additionally, when URE conducted dynamic studies of Category B contingencies as part of its Mitigation Plan, it confirmed that the system remains stable in the face of a Category B contingency.**

## 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) **6/18/07 (when the Standard became mandatory and enforceable) through 11/13/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

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-07-2552** |
| DATE SUBMITTED TO REGIONAL ENTITY | **5/27/10 (signed 5/26/10)** |
| DATE ACCEPTED BY REGIONAL ENTITY | **5/27/10** |
| DATE APPROVED BY NERC | **6/25/10** |
| DATE PROVIDED TO FERC | **6/28/10** |

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 **11/13/09**

DATE OF CERTIFICATION LETTER **6/2/10 (signed 5/28/10)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **11/13/09**

DATE OF VERIFICATION LETTER **7/30/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **11/13/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE reviewed and revised the rationale it used to identify and select Category B contingencies for study. URE conducted dynamic studies of Category B contingencies to determine whether such events would affect the stability of the system, and did not identify any Category B contingencies that would result in system instability. URE revised its TPL-002 assessment practices, rationale, and methodology for selecting Category B contingency events. Under its revised practices and procedures, URE will perform annual assessments and include dynamic simulations of generator bus faults in all necessary future system studies.**

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 Transmission System long-term plan**

EXHIBITS:

SOURCE DOCUMENT
**Reliability*First*'s Public Audit Report**

MITIGATION PLAN
**Mitigation Plan submitted May 27, 2010**

CERTIFICATION BY REGISTERED ENTITY
**Certification of Mitigation Plan Completion submitted June 2, 2010**

VERIFICATION BY REGIONAL ENTITY
**Verification of Mitigation Plan Completion dated July 30, 2010**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for TPL-003-0 R1

# DISPOSITION OF VIOLATION
## Dated September 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC200900154** | **RFC200900154** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **TPL-003-0** | **1** | **1.3, 1.3.1, 1.3.7** | **High**[1] | **Severe** |

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

**The purpose statement of TPL-003-0 provides: "System simulations and associated assessments are needed periodically to ensure that reliable systems are developed that meet specified performance requirements, with sufficient lead time and continue to be modified or upgraded as necessary to meet present and future System needs."**

**TPL-003-0 R1 provides in pertinent part:**

> **R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission systems is planned such that the network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand Levels over the range of forecast system demands, under the contingency conditions as defined in Category C of Table I (attached). The controlled interruption of customer Demand, the planned removal of generators, or the Curtailment of firm (non-recallable reserved) power transfers may be necessary to meet this standard. To be valid, the Planning Authority and Transmission Planner assessments shall:**
>
> **…**
>
> **R1.3. Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category C of Table 1 (multiple contingencies). The specific elements selected (from each of the following categories) for inclusion in**

[1] TPL-003-1 R1 has a High Violation Risk Factor (VRF) and its sub-requirements have Medium VRFs.

**these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).**

**R1.3.1. Be performed and evaluated only for those Category C contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.**

**…**

**R1.3.7. Demonstrate that System performance meets Table 1 for Category C contingencies.**

VIOLATION DESCRIPTION

**During an on-site audit of URE, the Reliability*First* audit team (Audit Team) determined that URE failed to demonstrate that system performance met Category C contingencies. The Audit Team reviewed the contingency files used in URE's 2008 study and determined that URE included all Category C single contingencies. Nevertheless, URE did not provide a statement that the system is stable as required by Table 1 for Category C contingencies, or that dynamic simulations were completed with the applicable seasonal assessments.**

**URE did not provide evidence that it conducted studies to establish that its voltage limits were within the applicable ratings for Category C contingencies. URE stated in its long term plans that only DC analysis was used for double contingencies due to the extensive contingency lists. URE could not establish that it could maintain voltages within applicable limits for Category C contingencies by using a DC load flow.**

**URE provided an attestation from two of its Managers, stating that there have been no significant changes to the URE system since 2002. In 2003, URE performed a dynamic study. URE's dynamic study for the 2004 summer peak, which included transient stability simulations of close in Category D faults at two URE generating stations, demonstrated that the generators remained stable for close in three phase faults with backup clearing. URE did not simulate all Category C contingencies in this study.**

**In 2007, URE's Planning Authority performed dynamic studies in which URE participated. The 2007 study stated that its purpose was to evaluate the dynamic stability of the Reliability Coordinator system in 2013 summer under various disturbances. The study also stated that the system was analyzed with the system intact and with 50 Category B, 139 Category C, and 79 Category D disturbances.**

**These disturbances were provided by Transmission Owners or selected from previous studies. No URE Category C contingencies were analyzed in this report. URE did not provide a rationale for the Category C contingencies selected for evaluation or an explanation of why the remaining simulations would produce less severe system results.**

**The Planning Authority also performed a generation interconnection study for a proposed hydro generation interconnection to the URE System.**

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

**Reliability*First* determined that this violation did not pose a substantial risk to the bulk power system because, although URE did not perform Category B or Category C contingency studies, URE did perform Category D contingency studies. Power Flow studies of the URE system demonstrate that a Category B or Category C contingency event that might result from an incorrect Facility Rating creates no overloads or voltage problems that URE could not quickly correct by switching, redispatching generation, or shedding local load. Further, the Power Flow studies demonstrate that the Category D extreme contingencies studied would not result in instability leading to a cascade. Additionally, when URE conducted dynamic studies of Category C contingencies as part of its Mitigation Plan, it confirmed that the system remains stable in the face of a Category C contingency.**

## 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) **6/18/07 (when the Standard became mandatory and enforceable) through 11/13/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

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-07-2553**
DATE SUBMITTED TO REGIONAL ENTITY **5/27/10 (signed 5/26/10)**
DATE ACCEPTED BY REGIONAL ENTITY **5/27/10**
DATE APPROVED BY NERC **6/25/10**
DATE PROVIDED TO FERC **6/28/10**

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 **11/13/09**

DATE OF CERTIFICATION LETTER **6/2/10 (signed 5/28/10)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **11/13/09**

DATE OF VERIFICATION LETTER **7/30/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **11/13/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE revised its rationale to ensure that all studies would include Category C contingencies that would produce the most severe system results using both AC and DC analyses, and both steady state and dynamic studies. URE conducted dynamic studies of Category C contingencies to determine whether such events would affect the stability of the system, and did not identify any Category C contingencies that would result in system instability.**

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 Transmission System long-term plan.**

EXHIBITS:

SOURCE DOCUMENT
**Reliability*First*'s Public Audit Report**

MITIGATION PLAN
**Mitigation Plan submitted May 27, 2010**

CERTIFICATION BY REGISTERED ENTITY
**Certification of Mitigation Plan Completion submitted June 2, 2010**

VERIFICATION BY REGIONAL ENTITY
**Verification of Mitigation Plan Completion dated July 30, 2010**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-003-1 R4

# DISPOSITION OF VIOLATION
## Dated September 10, 2010

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **RFC201000236** | **RFC201000236** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-003-1[1]** | **4** | | **Medium[2]** | **Moderate** |

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[3] 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…" (footnote added)**

**CIP-003-1 R4 provides:**

> **R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.**
>
> **R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.**
>
> **R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.**

[1] CIP-003-1 was enforceable from July 1, 2008 for Table 1 entities with Critical Cyber Assets in its System Control Center through March 31, 2010. CIP-003-2 is the current enforceable Standard as of April 1, 2010.
[2] CIP-003-1 R4 and R4.1 have a Medium Violation Risk Factor (VRF); R4.2 and R4.3 each have a Lower VRF.
[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.

**R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.**

VIOLATION DESCRIPTION

**On February 1, 2010, URE self-reported a violation on CIP-003-1 R4 for its failure to implement its program to classify information associated with Critical Cyber Assets based on the sensitivity of that information. On January 26, 2010, URE discovered that on October 5, 2009, it created a network folder, designated to contain CIP-confidential information in a manner that provided any URE employee with read-only access to the network folder's contents.**

**On January 26, 2010, URE limited the access rights to this network folder and commenced a review of the user access log for this network folder. URE determined that only two unauthorized persons had actually accessed the network folder. Both were current URE employees seeking an internal transfer into the NERC compliance group, who had accessed the network folder in preparation for their interviews.**

**In addition, on January 26, 2010, URE initiated a detailed review of all of its network folders that are categorized as potentially containing CIP-related information. Based on this detailed review, URE determined that this was an isolated case, and that all other NERC confidential directories were appropriately configured for restricted access.**

**On April 21, 2010, URE performed a root cause analysis and determined that the lack of a formal process and training for those involved with network folder creation and movement caused the violation.**

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 because only two persons actually accessed the folder in question and both were full-time URE employees seeking an internal transfer into URE's NERC compliance group. Furthermore, although the network folder contained information marked as CIP confidential material, URE determined upon further review that the information was improperly classified as CIP confidential material; thus, there was no CIP confidential or sensitive information on the folder. Additionally, URE determined that this was an isolated case, and that all other NERC confidential directories were appropriately configured for restricted access.**

## 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) **10/5/09 (when URE created the network folder) through 2/1/10 (when URE corrected the access controls on the folder and put a control process in place)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **2/1/10**

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-10-2563** |
| DATE SUBMITTED TO REGIONAL ENTITY | **6/10/10** |
| DATE ACCEPTED BY REGIONAL ENTITY | **6/18/10** |
| DATE APPROVED BY NERC | **6/30/10** |
| DATE PROVIDED TO FERC | **6/30/10** |

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 | **5/5/10** |

DATE OF CERTIFICATION LETTER **6/22/10 (signed 6/21/10)**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **5/5/10**

DATE OF VERIFICATION LETTER **7/13/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **5/5/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE applied the appropriate access controls and restricted access to the folder, and implemented an initial process to ensure that all access controls are properly managed by IT. URE documented an enhanced process for folder creation and changes associated with NERC compliance files, trained employees on the new process, and implemented the new process.**

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)

- **an e-mail with a subject "NERC CIP Folder Structure" dated January 26, 2010, which stated that the group "everyone" was removed from the folder in question which restored access to only the authorized individuals.**
- **an e-mail with a subject "Creation of LAN Directories for Compliance use," in which instructions were given that any new directory creation or folder movement was to be handled by IT personnel and not the Compliance personnel. URE continued to enhance the process and finally implemented processes for NERC Compliance team members.**
- **an e-mail with requested root cause documents. The conclusion of the root cause analysis was that the roles and responsibilities of the NERC Compliance personnel and the IT personnel needed to be defined and training needed to be provided to both groups.**
- **Training materials and attendance sheets that indicated the IT personnel were trained on May 4, 2010 and NERC Compliance personnel were trained on April 30, May 3, and May 5, 2010.**

EXHIBITS:

SOURCE DOCUMENT
**Self-Report dated February 1, 2010**

MITIGATION PLAN
**Mitigation Plan dated June 10, 2010**

CERTIFICATION BY REGISTERED ENTITY
**Certification of Mitigation Plan Completion dated June 22, 2010**

VERIFICATION BY REGIONAL ENTITY
**Verification of Mitigation Plan Completion dated July 13, 2010**