PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

August 31, 2011

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Documents attached thereto, 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 Southwest Power Pool Regional Entity (SPP RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SPP RE's determination and findings of the violations of CIP-002-1 Requirement(R)1 and R3, CIP-003-1 R1, CIP-004-1 R2, R3, and R4, CIP-007-1 R5, CIP-008-1 R1, and CIP-009-1 R2. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of eight thousand dollars ($8,000), 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 SPP200900146,

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

[2] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

SPP201000309, SPP201000310, SPP201000311, SPP201000312, SPP201000313, SPP201000314, SPP201000315, SPP201000316 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 August 25, 2011, by and between SPP RE 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-887 | SPP200900146 | CIP-002-1 | 1 | Lower[3] | 7/1/08-4/13/10 | 8,000 |
| | SPP201000309 | CIP-002-1 | 3 | High[4] | | |
| | SPP201000310 | CIP-003-1 | 1 | Medium[5] | | |
| | SPP201000311 | CIP-004-1 | 2 | Medium[6] | | |

[3] CIP-002-1 R1 and R1.2 each are assigned a "Medium" Violation Risk Factor (VRF) and CIP-002-1 R1.2, R1.2.1, R1.2.2, R1.2.3, R1.2.4, R1.2.5, R1.2.6 and R1.2.7 are each assigned a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-002-1 R1 and R1.2 "Lower" VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRFs and on January 27, 2009, the Commission approved the modified "Medium" VRFs. Therefore, the "Lower" VRFs for CIP-002-1 R1 and R1.2 were in effect from June 18, 2007 until January 27, 2009 when the "Medium" VRFs became effective.

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

[5] CIP-003-1 R1 has a "Medium" VRF; R1.1, R1.2 and R1.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-003-1 R1 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-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[6] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" VRF; R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


| | | | | | | |
|---|---|---|---|---|---|---|
| | SPP201000312 | CIP-004-1 | 3 | Medium[7] | | |
| | SPP201000313 | CIP-004-1 | 4 | Lower[8] | | |
| | SPP201000314 | CIP-007-1 | 5 | Medium[9] | | |
| | SPP201000315 | CIP-008-1 | 1 | Lower | | |
| | SPP201000316 | CIP-009-1 | 2 | Lower | | |

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

CIP-002-1 R1- OVERVIEW

During a Spot Check, SPP RE determined that URE did not comply with this standard. Specifically, URE's Risk Based Assessment Methodology (RBAM) did not (i) include the evaluation criteria used in identifying its Critical Assets as specified in sub-requirement R1.1 and (ii) consider each of the required asset categories listed in sub-requirements R1.2.1 through R1.2.7.

CIP-002-1 R3- OVERVIEW

During a Spot Check, SPP RE determined that URE failed to remove a laptop computer from its Critical Cyber Asset (CCA) list when the laptop computer was repurposed and no longer considered to be a CCA.

CIP-003-1 R1- OVERVIEW

During a Spot Check, SPP RE determined that URE had a possible violation of this Standard because: (i) URE's Cyber Security Policy did not provide for emergency situations as required by R1.1, (ii) URE's Cyber Security Policy was not readily available to its Energy Management System (EMS)/Supervisory Control and Data Acquisition (SCADA) vendor as required by R1.2,

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

[8] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF. When NERC filed 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.

[9] CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, R5.2.2, R5.3, R5.3.1 and R5.3.2 each have a Lower VRF; R5.1, R5.1.3, R5.2.1 and R5.2.3 each have a Medium VRF. When NERC filed VRFs it originally assigned CIP-007-1 R5.1, R5.1.3, R5.2.1, R5.2.3 and R5.3.3 "Lower" VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRFs and on February 2, 2009 and August 20, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-007-1 R5.1.3, R5.2.1, R5.2.3 were in effect from June 18, 2007 until February 2, 2009, when the "Medium" VRFs became effective and the "Lower" VRFs for CIP-007-1 R5.1 and R5.3.3 were in effect from June 18, 2007 until August 20, 2009, when the "Medium" VRFs became effective.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


and (iii) URE's Cyber Security Policy allowed for acceptance of risk, training to be conducted within 90 days of receiving access to URE's CCAs, and a Personnel Risk Assessment to be conducted within 30 days of receiving access to URE's CCAs.

CIP-004-1 R2- OVERVIEW

During a Spot Check, SPP RE determined that URE had a possible violation of this Standard because URE's EMS/SCADA vendor personnel were not trained in URE's cyber security policies as required by R2.1.

CIP-004-1 R3- OVERVIEW

During a Spot Check, SPP RE determined that URE had a possible violation of CIP-004-1 R3. Specifically, the SPP RE determined that URE violated sub-requirement R3.3 because: (i) URE did not conduct its personnel risk assessments pursuant to its documented personnel risk assessment program within 30 days of personnel being granted authorized cyber or authorized unescorted physical access to CCAs, (ii) URE did not conduct its personnel risk assessment pursuant to its documented personnel risk assessment program prior to personnel being granted authorized cyber or authorized unescorted physical access, and (iii) URE did not document that each EMS/SCADA vendor conducted these assessments.

CIP-004-1 R4- OVERVIEW

During a Spot Check, SPP RE determined that URE had a possible violation of CIP-004-1 R4.1 because URE did not maintain a complete list of personnel with authorized cyber or authorized unescorted physical access to CCAs. URE's access list also failed to include the specific electronic and physical access rights that its personnel and EMS/SCADA vendors had to its CCAs. URE also could not provide evidence that the EMS/SCADA vendor access list had been reviewed quarterly as required by the Standard.

CIP-007-1 R5- OVERVIEW

During a Spot Check, SPP RE determined that URE had a possible violation of CIP-007-1 R5. Specifically, the SPP RE determined that URE was in violation of sub-requirement R5.2.3 because a shared user account was not secured by changing the password or by other means when a dispatcher with authorized access retired. URE was also found to be in violation of sub-requirement R5.3.3 because a password was identified that had not been changed at least annually.

CIP-008-1 R1- OVERVIEW

During a Spot Check, SPP RE determined that URE had a possible violation of CIP-008-1 R1. Specifically, URE had a possible violation of sub-requirements R1.2, R1.5 and R1.6 because: (i) the roles and responsibilities of its incident response team members were not defined (R1.2), (ii) URE lacked evidence that it reviewed its incident response plan in 2008 (R1.5), and (iii) URE could not provide evidence that it tested its incident response plan annually (R1.6).

CIP-009-1 R2- OVERVIEW

During a Spot Check, SPP RE determined that URE could not provide evidence that it performed an annual exercise of its recovery plan.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


**Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed**[10]

**Basis for Determination**

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines, the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[11] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on August 2, 2011. The NERC BOTCC approved the Settlement Agreement, including SPP RE's assessment of an eight thousand dollar ($8,000) 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:[12]

1. the violations constituted URE's first occurrence of violation of the subject NERC Reliability Standards;
2. SPP RE reported that URE was cooperative throughout the compliance enforcement process;
3. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
4. SPP RE determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), as discussed in the Disposition Documents; and
5. SPP RE reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of eight thousand dollars ($8,000) 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.

[10] *See* 18 C.F.R. § 39.7(d)(4).
[11] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).
[12] URE did not receive credit for having a compliance program because it does not have a documented compliance program.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

**Attachments to be included as Part of this Notice of Penalty**

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

a) Settlement Agreement by and between SPP RE and URE executed August 25, 2011, included as Attachment a;

   i. Disposition Document for Common Information, included as Attachment 1 to the Settlement Agreement;

   ii. Disposition Document for CIP-002-1 R1 included as Attachment 1a to the Settlement Agreement; and

   iii. Disposition Document for CIP-002-1 R3, CIP-003-1 R1, CIP-004-1 R2- R4, CIP-007-1 R5, CIP-008-1 R1 and CIP-009-1 R2 included as Attachment 1b to the Settlement Agreement;

b) SPP RE's Public Source Document for CIP-002-1 R1, included as Attachment b;

c) SPP RE's Public Source Document for CIP-002-1 R3, CIP-003-1 R1, CIP-004-1 R2- R4, CIP-007-1 R5, CIP-008-1 R1 and CIP-009-1 R2, included as Attachment c;

d) URE'S Mitigation Plan MIT-08-2918 for CIP-002-1 R1, included as Attachment d;

e) URE'S Mitigation Plan MIT-08-3264 for CIP-002-1 R3, included as Attachment e;

f) URE'S Mitigation Plan MIT-08-3265 for CIP-003-1 R1, included as Attachment f;

g) URE'S Mitigation Plan MIT-08-3266 for CIP-004-1 R2, included as Attachment g;

h) URE'S Mitigation Plan MIT-08-3267 for CIP-004-1 R3, included as Attachment h;

i) URE'S Mitigation Plan MIT-08-3268 for CIP-004-1 R4, included as Attachment i;

j) URE'S Mitigation Plan MIT-08-3269 for CIP-007-1 R5, included as Attachment j;

k) URE'S Mitigation Plan MIT-08-3270 for CIP-008-1 R1, included as Attachment k;

l) URE'S Mitigation Plan MIT-08-3271 for CIP-009-1 R2, included as Attachment l;

m) URE's Certification of Mitigation Plan Completion for MIT-08-2918, included as Attachment m;

n) URE's Certification of Completed Mitigation Plans for MIT-08-3264, MIT-08-3265, MIT-08-3266, MIT-08-3267, MIT-08-3268, MIT-08-3269, MIT-08-3270, and MIT-08-3271 , included as Attachment n;

o) SPP RE's Mitigation Plan Completion Notice for MIT-08-2918, included as Attachment o; and

p) SPP RE's Mitigation Plan Completion Notice for MIT-08-3264, MIT-08-3265, MIT-08-3266, MIT-08-3267, MIT-08-3268, MIT-08-3269, MIT-08-3270, and MIT-08-3271, included as Attachment p.

**A Form of Notice Suitable for Publication**[13]

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

[13] *See* 18 C.F.R. § 39.7(d)(6).

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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>*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. | Rebecca J. Michael*<br>Associate General Counsel for Corporate and Regulatory Matters<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>Stacy Dochoda*<br>General Manager<br>Southwest Power Pool Regional Entity<br>16101 La Grande, Ste 103<br>Little Rock, AR 72223<br>(501) 688-1730<br>(501) 821-8726 – facsimile<br>sdochoda.re@spp.org<br><br>Joe Gertsch*<br>Manager of Enforcement<br>Southwest Power Pool Regional Entity<br>16101 La Grande, Ste 103<br>Little Rock, AR 72223<br>(501) 688-1672<br>(501) 821-8726 – facsimile<br>jgertsch.re@spp.org<br><br>Machelle Smith*<br>Paralegal & SPP RE File Clerk<br>Southwest Power Pool Regional Entity<br>16101 La Grande, Ste 103<br>Little Rock, AR 72223<br>(501) 688-1681<br>(501) 821-8726 – facsimile<br>spprefileclerk @spp.org |

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

**Conclusion**

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

Respectfully submitted,

/s/ *Rebecca J. Michael*

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

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

cc: Unidentified Registered Entity
Southwest Power Pool Regional Entity

Attachments

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for Common Information

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

# DISPOSITION OF VIOLATION[1]

**INFORMATION COMMON TO INSTANT VIOLATIONS**
**Dated August 25, 2011**

| REGISTERED ENTITY | NERC REGISTRY ID | NOC# |
|---|---|---|
| **Unidentified Registered Entity (URE)** | **NCRXXXXX** | **NOC-887** |

REGIONAL ENTITY
**Southwest Power Pool Regional Entity (SPP RE)**

IS THERE A SETTLEMENT AGREEMENT YES ☒ NO ☐

WITH RESPECT TO THE VIOLATION(S), REGISTERED ENTITY

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

WITH RESPECT TO THE ASSESSED PENALTY OR SANCTION, REGISTERED ENTITY

ACCEPTS IT/ DOES NOT CONTEST IT YES ☒

## I. PENALTY INFORMATION

TOTAL ASSESSED PENALTY OR SANCTION OF **$8,000** FOR **NINE** VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

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

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

**URE's internal compliance program is not documented.**

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

**See above.**

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

YES ☐ NO ☒
IF YES, EXPLAIN

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


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

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

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

SETTLEMENT DISCUSSIONS COMMENCED
**SPP200900146**
DATE: **7/21/10** OR N/A ☐

**SPP201000309_310_311_312_313_314_315_316**
DATE: **1/14/11**

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

SUPPLEMENTAL RECORD INFORMATION
DATE(S) OR N/A ☒
REGISTERED ENTITY RESPONSE CONTESTED
FINDINGS ☐ PENALTY ☐ BOTH ☐ DID NOT CONTEST ☐

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


HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-002-1 R1

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

Attachment 1a

# DISPOSITION OF VIOLATION

**Dated August 25, 2011**

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **SPP200900146** | **2009-076** |

## I. VIOLATION INFORMATION

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

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

**The purpose statement of CIP-002-1 provides:**

> **Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.**

**CIP-002-1 R1 provides:**

> **R1. Critical Asset Identification Method — The Responsible Entity[3] shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.**
>
> > **R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.**

[1] CIP-002-1 R1 and R1.2 each are assigned a "Medium" Violation Risk Factor (VRF) and CIP-002-1 R1.2, R1.2.1, R1.2.2, R1.2.3, R1.2.4, R1.2.5, R1.2.6 and R1.2.7 are each assigned a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-002-1 R1 and R1.2 "Lower" VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRFs and on January 27, 2009, the Commission approved the modified "Medium" VRFs. Therefore, the "Lower" VRFs for CIP-002-1 R1 and R1.2 were in effect from June 18, 2007 until January 27, 2009 when the "Medium" VRFs became effective.

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

[3] Within the text of Standard CIP-002-1, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC and Regional Reliability Organizations.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


**R1.2. The risk-based assessment shall consider the following assets:**

**R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.**

**R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.**

**R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.**

**R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.**

**R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.**

**R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.**

**R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment**.

**(Footnote added.)**

VIOLATION DESCRIPTION

**During a CIP Compliance Spot Check of the Unidentified Registered Entity (URE), the SPP RE Audit Team found that URE was not compliant with CIP-002-1 R1. Specifically, URE's Risk Based Assessment Methodology (RBAM) did not include the evaluation criteria used in identifying its Critical Assets and URE's RBAM did not reference or consider each of the required asset categories listed in sub-requirements R1.2.1 through R1.2.7.**

RELIABILITY IMPACT STATEMENT – POTENTIAL AND ACTUAL

**The SPP RE has determined that URE's violation of CIP-002-1 R1 did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). In the**

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


**course of revising its RBAM, URE adopted modified procedures and evaluation criteria for identifying Critical Assets. URE subsequently applied the modified procedures and evaluation criteria and determined that it does not own or operate any systems, facilities, and/or equipment that, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BPS. Subsequent to the revision of its RBAM, URE determined that it had incorrectly identified Critical Assets in its original RBAM, and did not, prior to the revision or now, have any Critical Assets.**

**Moreover, URE does not own or operate any transmission or distribution facilities. URE does not own generation. Thus, as documented in its revised RBAM, URE has minimal BPS systems, facilities, and/or equipment that could be considered as candidate Critical Assets and no systems, facilities, or equipment capable of impacting the reliability or operability of the BPS.**

## 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 through 4/13/10 (Mitigation Plan completion)**

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

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

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


## III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

| | |
|---|---|
| MITIGATION PLAN NO. | **MIT-08-2918** |
| DATE SUBMITTED TO REGIONAL ENTITY | **7/2/10** |
| DATE ACCEPTED BY REGIONAL ENTITY | **10/6/10** |
| DATE APPROVED BY NERC | **10/6/10** |
| DATE PROVIDED TO FERC | **10/26/10** |

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

| | |
|---|---|
| EXPECTED COMPLETION DATE | **4/31/10**[4] |
| EXTENSIONS GRANTED | **None** |
| ACTUAL COMPLETION DATE | **4/13/10** |

| | |
|---|---|
| DATE OF CERTIFICATION LETTER | **10/20/10**[5] |
| CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF | **4/13/10** |

| | |
|---|---|
| DATE OF VERIFICATION LETTER | **10/19/10** |
| VERIFIED COMPLETE BY REGIONAL ENTITY AS OF | **4/13/10** |

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE revised its RBAM to clearly reflect evaluation criteria as required by sub-requirement R1.1 and include all asset categories specified in sub-requirement R1.2. URE utilized NERC's official guidance regarding the identification of Critical Assets when revising its RBAM. (*See* NERC Security Guideline for the Electricity Sector: Identifying Critical Assets (Version 1.0, eff. Sept. 17, 2009).)**

**Following the revision of its RBAM, URE applied the modified evaluation criteria to its candidate Critical Assets within the asset categories listed in sub-requirements 1.2.1 through 1.2.7 of CIP-002-1 R1. After assessing whether its candidate Critical Assets could affect the reliability or operability of the BPS if destroyed, degraded, or rendered unavailable according to its evaluation criteria, URE determined that it did not have any Critical Assets.**

[4] The Mitigation Plan incorrectly stated that the proposed completion date was March 31, 2010.
[5] The Certification of Completion for Mitigation Plan SPP200900146 was amended on October 20, 2010, due to clerical error and date discrepancy. The SPP RE had sufficient evidence to verify mitigation plan completion on October 19, 2010.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


**URE's revised RBAM and its Critical Asset assessment were found by the SPP RE to be compliant at a later Spot Check, which was conducted on-site at URE's offices.**

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 revised RBAM**
- **Letter of Attestation from a URE manager regarding the revised RBAM**
- **URE RBAM Asset Review List**

EXHIBITS:

SOURCE DOCUMENT
**SPP RE's Public Source Document**

MITIGATION PLAN
**URE'S Mitigation Plan MIT-08-2918**

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

VERIFICATION BY REGIONAL ENTITY
**SPP RE's Mitigation Plan Completion Notice**

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Disposition Document for CIP-002-1 R3, CIP-003-1 R1, CIP-004-1 R2- R4, CIP-007-1 R5, CIP-008-1 R1 and CIP-009-1 R2

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION



# DISPOSITION OF VIOLATION
## Dated August 25, 2011

| NERC TRACKING NO. | REGIONAL ENTITY TRACKING NO. |
|---|---|
| **SPP201000309** | **2010-115** |
| **SPP201000310** | **2010-116** |
| **SPP201000311** | **2010-117** |
| **SPP201000312** | **2010-118** |
| **SPP201000313** | **2010-119** |
| **SPP201000314** | **2010-120** |
| **SPP201000315** | **2010-121** |
| **SPP201000316** | **2010-122** |

## I. VIOLATION INFORMATION

| RELIABILITY STANDARD | REQUIREMENT(S) | SUB-REQUIREMENT(S) | VRF(S) | VSL(S) |
|---|---|---|---|---|
| **CIP-002-1** | **3** | | **High**[1] | **N/A**[2] |
| **CIP-003-1** | **1** | **1.1, 1.2** | **Medium**[3] | **N/A** |
| **CIP-004-1** | **2** | **2.1** | **Medium**[4] | **N/A** |
| **CIP-004-1** | **3** | **3.3** | **Medium**[5] | **N/A** |

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

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

[3] CIP-003-1 R1 has a "Medium" VRF; R1.1, R1.2 and R1.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-003-1 R1 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-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[4] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" VRF; R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[5] CIP-004-1 R3 has a "Medium" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower"

| | | | | |
|---|---|---|---|---|
| **CIP-004-1** | **4** | **4.1** | **Lower**[6] | **N/A** |
| **CIP-007-1** | **5** | **5.2.3, 5.3.3** | **Medium**[7] | **N/A** |
| **CIP-008-1** | **1** | **1.2, 1.5, 1.6** | **Lower** | **N/A** |
| **CIP-009-1** | **2** | | **Lower** | **N/A** |

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

**The purpose statement of CIP-002-1 provides in pertinent part:**

> **Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.**

**CIP-002-1 R3 provides:**

> **R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity[8] shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall**

---

VRF for CIP-004-1 R3 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[6] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF. When NERC filed 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.

[7] CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, R5.2.2, R5.3, R5.3.1 and R5.3.2 each have a Lower VRF; R5.1, R5.1.3, R5.2.1 and R5.2.3 each have a Medium VRF. When NERC filed VRFs it originally assigned CIP-007-1 R5.1, R5.1.3, R5.2.1, R5.2.3 and R5.3.3 "Lower" VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRFs and on February 2, 2009 and August 20, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-007-1 R5.1.3, R5.2.1, R5.2.3 were in effect from June 18, 2007 until February 2, 2009, when the "Medium" VRFs became effective and the "Lower" VRFs for CIP-007-1 R5.1 and R5.3.3 were in effect from June 18, 2007 until August 20, 2009, when the "Medium" VRFs became effective.

[8] Within the text of Standard CIP-002-1 through CIP-009-1, "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

> **review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:**
>
> > **R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,**
> >
> > **R3.2. The Cyber Asset uses a routable protocol within a control center; or,**
> >
> > **R3.3. The Cyber Asset is dial-up accessible.**

**(Footnote added.)**

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

**CIP-003-1 R1 provides in pertinent part:**

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

**The purpose of CIP-004-1 provides in pertinent part:**

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

**CIP-004-1 provides in pertinent part:**

> **R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.**
>
> > **R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.**
> >
> > **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.**
>
> **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 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.**

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

**Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.**

**CIP-007-1 R5 provides in pertinent part:**

**R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.**

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

**R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.**

**The purpose 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 shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:**

**R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.**
**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.**

**The purpose of CIP-009-1 provides in pertinent part:**

**Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard**

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


**CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.**

**CIP-009-1 R2 provides: "Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident."**

VIOLATION DESCRIPTIONS

**CIP-002-1 R3 SPP201000309: During a Spot Check (the "Spot Check"), the SPP RE found that the Unidentified Registered Entity (URE) had a possible violation of CIP-002-1 R3 because URE failed to remove a laptop computer from its Critical Cyber Asset (CCA) list when the laptop computer was repurposed and no longer considered to be a CCA. This possible violation was based upon the identification of Critical Assets and CCAs by URE utilizing its 2009 Risk Based Assessment Methodology (original RBAM). URE subsequently adopted a revised version of its RBAM (2010) and its Critical Asset/CCA assessment and corresponding asset lists (collectively, the revised RBAM). As documented in the revised RBAM, URE does not own Critical Assets or CCAs subject to the NERC CIP Reliability Standards.**

**CIP-003-1 R1 SPP201000310: During the Spot Check, the SPP RE found that URE had a possible violation of CIP-003-1 R1.1 and CIP-003-1 R1.2 because: (i) URE's Cyber Security Policy did not provide for emergency situations as required by R1.1, (ii) URE's Cyber Security Policy was not readily available to its Energy Management System (EMS)/Supervisory Control and Data Acquisition (SCADA) vendor as required by R1.2, and (iii) URE's Cyber Security Policy did not address changes from Version 1 to Version 2 of the CIP Standards (specifically URE's Cyber Security Policy continued to allow for acceptance of risk, training to be conducted within 90 days of receiving access to URE's CCAs, and a Personnel Risk Assessment to be conducted within 30 days of receiving access to URE's CCAs). This possible violation was based upon the identification of Critical Assets and CCAs by URE utilizing the original RBAM. As documented in the revised RBAM, URE does not own Critical Assets or CCAs subject to the NERC CIP Reliability Standards.**

**CIP-004-1 R2 SPP201000311: During the Spot Check, the SPP RE found that URE had a possible violation of CIP-004-1 R2 and CIP-004-2 R2 because URE's EMS/SCADA vendor personnel were not trained in URE's cyber security policies as required by R2.1. This possible violation was based upon the identification of Critical Assets and CCAs by URE utilizing the original RBAM. As documented in the revised RBAM, URE does not own Critical Assets or CCAs subject to the NERC CIP Reliability Standards.**

**CIP-004-1 R3 SPP201000312: During the Spot Check, the SPP RE found that URE had a possible violation of CIP-004-1 R3 and CIP-004-2 R3. Specifically, the SPP RE determined that URE violated sub-requirement R3.3 because: (i) URE did not**

**conduct its personnel risk assessments pursuant to its documented personnel risk assessment program within 30 days of personnel being granted authorized cyber or authorized unescorted physical access to CCAs and (ii) URE did not conduct its personnel risk assessment pursuant to its documented personnel risk assessment program prior to personnel being granted authorized cyber or authorized unescorted physical access., and (iii) URE did not document that each EMS/SCADA vendor conducted these assessments. This possible violation was based upon the identification of Critical Assets and CCAs by URE utilizing the original RBAM. As documented in the revised RBAM, URE does not own Critical Assets or CCAs subject to the NERC CIP Reliability Standards.**

**CIP-004-1 R4 SPP201000313: During the Spot Check, the SPP RE found that URE had a possible violation of CIP-004-1 R4 and CIP-004-2 R4. Specifically, the SPP RE found that URE was in violation of sub-requirement R4.1 because URE did not maintain a complete list of personnel with authorized cyber or authorized unescorted physical access to CCAs. URE's access list also failed to include the specific electronic and physical access rights that its personnel and EMS/SCADA vendors had to its CCAs. URE also could not provide evidence that the EMS/SCADA vendor access list had been reviewed quarterly as required by the Standard. This possible violation was based upon the identification of Critical Assets and CCAs by URE utilizing the original RBAM. As documented in the revised RBAM, URE does not own Critical Assets or CCAs subject to the NERC CIP Reliability Standards.**

**CIP-007-1 R5 SPP201000314: During the Spot Check, the SPP RE found that URE had a possible violation of CIP-007-1 R5 and CIP-007-2 R5. Specifically, the SPP RE determined that URE was in violation of sub-requirement R5.2.3 because a shared user account was not secured by changing the password or by other means when a dispatcher with authorized access retired. URE was also found to be in violation of sub-requirement R5.3.3 because a password was identified that had not been changed at least annually. This possible violation was based upon the identification of Critical Assets and CCAs by URE utilizing the original RBAM. As documented in the revised RBAM, URE does not own Critical Assets or CCAs subject to the NERC CIP Reliability Standards.**

**CIP-008-1 R1 SPP201000315: During the Spot Check, the SPP RE found that URE had a possible violation of CIP-008-1 R1 and CIP-008-2 R1. Specifically, URE had a possible violation of sub-requirements R1.2, R1.5 and R1.6 because: (i) the roles and responsibilities of its incident response team members were not defined (R1.2), (ii) URE lacked evidence that it reviewed its incident response plan in 2008 (R1.5), and (iii) URE could not provide evidence that it tested its incident response plan annually (R1.6). This possible violation was based upon the identification of Critical Assets and CCAs by URE utilizing the original RBAM. As documented in the revised RBAM, URE does not own Critical Assets or CCAs subject to the NERC CIP Reliability Standards.**

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


**CIP-009-1 R2 SPP201000316: During the Spot Check, the SPP RE found that URE had a possible violation of CIP-009-1 R2 and CIP-009-2 R2 because URE could not provide evidence that it performed an annual exercise of its recovery plan. This possible violation was based upon the identification of Critical Assets and CCAs by URE utilizing the original RBAM. As documented in the revised RBAM, URE does not own Critical Assets or CCAs subject to the NERC CIP Reliability Standards.**

RELIABILITY IMPACT STATEMENT – POTENTIAL AND ACTUAL

**The SPP RE has determined that URE's violations of the aforementioned standards did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Due to the revision of its RBAM as described in Attachment 1a, the violations identified herein have become moot.**

**In the course of revising its RBAM to mitigate the alleged violation of CIP-002-1 R1, URE adopted modified procedures and evaluation criteria for identifying Critical Assets. Subsequent to the revision of its RBAM, URE determined that it had incorrectly identified Critical Assets in its original RBAM and did not, prior to the revision or now have any Critical Assets.**

**Moreover, URE does not own or operate any transmission or distribution facilities. URE does not own generation. Thus, as documented in the revised RBAM, URE has minimal BPS systems, facilities, and/or equipment that could be considered as candidate Critical Assets and no systems, facilities, or equipment capable of impacting the reliability or operability of the BPS.**

## 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): **For all violations: 7/1/08 through 4/13/10 (Mitigation Plan completion)**

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


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. **CIP-002-1 R3: MIT-08-3264**
**CIP-003-1 R1: MIT-08-3265**
**CIP-004-1 R2: MIT-08-3266**
**CIP-004-1 R3: MIT-08-3267**
**CIP-004-1 R4: MIT-08-3268**
**CIP-007-1 R5: MIT-08-3269**
**CIP-008-1 R1: MIT-08-3270**
**CIP-009-1 R2: MIT-08-3271**

DATE SUBMITTED TO REGIONAL ENTITY **1/5/10**
DATE ACCEPTED BY REGIONAL ENTITY **1/11/11**
DATE APPROVED BY NERC **2/4/11**
DATE PROVIDED TO FERC **2/8/11**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **4/13/10**
EXTENSIONS GRANTED **None**
ACTUAL COMPLETION DATE **4/13/10**

DATE OF CERTIFICATION LETTER **1/6/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **4/13/10**

DATE OF VERIFICATION LETTER **2/17/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **4/13/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

**URE implemented a revised RBAM for the identification of Critical Assets and Critical Cyber Assets. The revised RBAM, which reflects an assessment methodology that is based upon and consistent with the guidance provided in**

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION


**the NERC Security Guideline for the Electricity Sector: Identifying Critical Assets (Version 1.0, eff. Sept. 17, 2009) included a documented assessment of the URE electric system to evaluate whether URE owns, operates, or controls Critical Assets or CCAs. According to the results of this assessment, no BPS facilities owned or operated by URE were identified as Critical Assets. Because URE does not own, operate, or control Critical Assets, URE has no corresponding CCAs. URE documented its null lists of Critical Assets and CCAs in the revised RBAM.**

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 revised RBAM**
- **Letter of Attestation from a URE manager regarding the revised RBAM**
- **URE RBAM asset review list**

EXHIBITS:

SOURCE DOCUMENT
**SPP RE's Public Source Document**

MITIGATION PLAN
**URE'S Mitigation Plan MIT-08-3264 for CIP-002-1 R3**
**URE'S Mitigation Plan MIT-08-3265 for CIP-003-1 R1**
**URE'S Mitigation Plan MIT-08-3266 for CIP-004-1 R2**
**URE'S Mitigation Plan MIT-08-3267 for CIP-004-1 R3**
**URE'S Mitigation Plan MIT-08-3268 for CIP-004-1 R4**
**URE'S Mitigation Plan MIT-08-3269 for CIP-007-1 R5**
**URE'S Mitigation Plan MIT-08-3270 for CIP-008-1 R1**
**URE'S Mitigation Plan MIT-08-3271 for CIP-009-1 R2**

CERTIFICATION BY REGISTERED ENTITY
**URE's Certification of Completed Mitigation Plans**

VERIFICATION BY REGIONAL ENTITY
**SPP RE's Mitigation Plan Completion Notice**