PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

October 7, 2010

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 an 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 a) and the Disposition Document (Attachment f), in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure, including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

On June 30, 2008, after being notified of an upcoming self-certification, URE submitted self-reports, which indicated that URE had not taken the necessary steps to comply with NERC Reliability Standards CIP-002-1 Requirement (R) 1, R2 and R3; CIP-003-1 R1, R2 and R3; CIP-004-1 R2, R3 and R4; CIP-007-1 R1; CIP-008-1 R1; and CIP-009-1 R1 and R2. During the compliance audit (Audit), SERC Compliance Audit Staff (SERC Staff) discovered that URE's Protection System[3] Maintenance and Testing Program document did not address each of the components of its transmission Protection System, as required by the standard, and during

[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).
[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."

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

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

SERC's Spot Check conducted from July 13, 2009 through July 14, 2009 (Spot Check), SERC determined that URE had a second violation of CIP-004-1 R2.1.

This NOP is being filed with the Commission because SERC and URE have entered into a Settlement Agreement to resolve all outstanding issues resulting in SERC's determination and findings of the enforceable violations of CIP-002-1 R1, R2 and R3; CIP-003-1 R1, R2 and R3; CIP-004-1 R2, R3 and R4; CIP-007-1 R1; CIP-008-1 R1; CIP-009-1 R1 and R2; and PRC-005-1 R1. According to the Settlement Agreement, URE neither admits nor denies the violation, but has agreed to the assessed penalty of sixteen thousand dollars ($16,000) 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.

Statement of Findings Underlying the Violations

This NOP incorporates the findings and justifications set forth in the Settlement Agreement executed on February 18, 2010, by and between SERC 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.

Region	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty ($)
SERC	SERC200800170	CIP-002-1	1	Medium	$16,000
	SERC200800171	CIP-002-1	2	High	
	SERC200800172	CIP-002-1	3	High[4]	
	SERC200800173	CIP-003-1	1	Medium	
	SERC200800174	CIP-003-1	2	Medium	
	SERC200800175	CIP-003-1	3	Lower	
	SERC200800176	CIP-004-1	2	Medium	
	SERC200800177	CIP-004-1	3	Medium	
	SERC200800178	CIP-004-1	4	Medium	
	SERC200800179	CIP-007-1	1	Medium[5]	
	SERC200800180	CIP-008-1	1	Lower	

[4] CIP-002-1 R3 has a "High" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF.
[5] CIP-007-1 R1 has a "Medium" VRF; R1.1, R1.2 and R1.3 each have a "Lower" VRF.

	SERC200800181	CIP-009-1	1	Medium	
	SERC200800182	CIP-009-1	2	Lower	
	SERC200800200	PRC-005-1	1	High[6]	
	SERC200900291	CIP-004-1	2.1	Medium	

The text of the Reliability Standards at issue is set forth in the Disposition Documents.

CIP-002-1 R1, R2 and R3 - OVERVIEW[7]
SERC determined that URE, as a Balancing Authority and Transmission Operator, did not have a risk-based methodology to identify Critical Assets as required by R1 and, therefore, did not have a list of Critical Assets as required by R2, and did not have a list of associated Critical Cyber Assets as required by R3.

The duration of the CIP-002-1 R1, R2 and R3 violations was from July 1, 2008, the date the Standard became mandatory and enforceable for Table 1[8] entities, through August 29, 2008, when URE completed its Mitigation Plan.

SERC concluded that this violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because after URE re-evaluated its risk-based methodology, it determined that it did not have any critical assets.[9] Also, URE is a small Balancing Authority with a low estimated summer peak.

CIP-003-1 R1, R2 and R3 - OVERVIEW[10]
SERC determined that URE, as a Balancing Authority and Transmission Operator, had a cyber security policy, but did not annually review or approve it, as required by R1, did not assign a senior manager as required by R2, and did not document exceptions as required by R3.

The duration of the CIP-003-1 R1 violation was from July 1, 2008, the date the Standard became mandatory and enforceable for Table 1 entities, through September 12, 2008, the date URE mitigated the violation by documenting and implementing its cyber security policy.

[6] When NERC filed Violation Risk Factors (VRFs) for PRC-005-1, NERC originally assigned a "Medium" VRF to PRC-005-1 R1. In the Commission's May 18, 2007 Order on VRFs, the Commission approved the VRF as filed, but directed modifications. On June 1, 2007, NERC filed a modified "High" VRF for PRC-005 R1 for approval. On August 9, 2007, the Commission issued an Order approving the modified VRF. Therefore, the "Medium" VRF was in effect from June 18, 2007, until August 9, 2007, and the "High" VRF has been in effect since August 9, 2007.
[7] Further information on this violation is contained in the Disposition Document included as Attachment f.1.
[8] *See Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1*.
[9] Initially, URE conservatively determined that certain assets were critical assets. Upon review and with the technical expertise of its consultant, URE determined that it had no critical assets (the loss of any elements would not impact the BPS), and thus no Critical Cyber Assets.
[10] Further information on this violation is contained in the Disposition Document included as Attachment f.1.

The duration of the CIP-003-1 R2 violation was from July 1, 2008, the date the Standard became mandatory and enforceable for Table 1 entities, through August 22, 2008, the date URE mitigated the violation by identifying a senior manager.

The duration of the CIP-003-1 R3 violation was from July 1, 2008, the date the Standard became mandatory and enforceable for Table 1 entities, through September 26, 2008, the date URE mitigated the violation by identifying any exceptions to its cyber security policy.

SERC concluded that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE is a small Balancing Authority with a low estimated summer peak and its Control Center Cyber Assets had only one external communications link, which was with its Reliability Coordinator.

CIP-004-1 R2, R3 and R4 - OVERVIEW[11]
SERC determined that URE, as a Balancing Authority and Transmission Operator, did not establish, maintain and document a cyber security training program as required by R2; implement and document a personnel risk assessment program as required by R3; and maintain list(s) of personnel with Critical Cyber Assets access rights as required by R4.

The duration of the CIP-004-1 R2 violation was from July 1, 2008, the date the Standard became mandatory and enforceable for Table 1 entities, through October 3, 2008, when URE completed its Mitigation Plan.

The duration of the CIP-004-1 R3 violation was from July 1, 2008, the date the Standard became mandatory and enforceable for Table 1 entities, through September 26, 2008, when URE completed its Personnel Risk Assessments.

The duration of the CIP-004-1 R4 violation was from July 1, 2008, the date the Standard became mandatory and enforceable for Table 1 entities, through August 29, 2008, when URE established its list of personnel with access to Critical Cyber Assets.

SERC concluded that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE is a small Balancing Authority with a low estimated summer peak and its Control Center cyber assets had only one external communications link, which was with its Reliability Coordinator.

Second Violation of CIP-004-1 R2.1 - OVERVIEW[12]
During the Spot Check, SERC staff determined that URE, as a Balancing Authority and Transmission Operator, although it had trained its new personnel under the prior Mitigation Plan, URE had not trained its existing staff, within ninety (90) days of July 1, 2008, the effective date of the Standard.

[11] Further information on this violation is contained in the Disposition Document included as Attachment f.2.
[12] Further information on this violation is contained in the Disposition Document included as Attachment f.2.

The duration of the CIP-004-1 R2.1 violation was from July 1, 2008, the date the Standard became mandatory and enforceable for Table 1 entities, through May 12, 2009, when URE completed training for its existing personnel.

SERC concluded that this violation of CIP-004-1 R2.1 for the gap in training did not pose a serious or substantial risk to the reliability of the BPS because the employees that did not receive the timely training were existing employees that had experience with URE's Critical Cyber Assets.

CIP-007-1 R1- OVERVIEW[13]
SERC determined that URE, as a Balancing Authority and Transmission Operator, did not create, implement and maintain test procedures to ensure existing cyber security controls were still in place after changes to Cyber Assets.

The duration of the CIP-007-1 R1 violation was from July 1, 2008, the date the Standard became mandatory and enforceable for Table 1 entities, through October 10, 2008, the date URE completed its Mitigation Plan.

SERC concluded that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE is a small Balancing Authority with a low estimated summer peak and its Control Center cyber assets had only one external communications link, which was with its Reliability Coordinator.

CIP-008-1 R1- OVERVIEW[14]
SERC determined that URE, as a Balancing Authority and Transmission Operator, did not develop and maintain a Cyber Security Incident response plan.

The duration of the CIP-008-1 R1 violation was from July 1, 2008, the date the Standard became mandatory and enforceable for Table 1 entities, through December 23, 2008, the date URE completed its Mitigation Plan.

SERC concluded that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE is a small Balancing Authority with a low estimated summer peak and its Control Center cyber assets had only one external communications link, which was with its Reliability Coordinator.

CIP-009-1 R1 and R2- OVERVIEW[15]
SERC determined that URE, as a Balancing Authority and Transmission Operator, did not create and annually review recovery plans for Critical Cyber Assets as required by R1 and, therefore, did not exercise its recovery plans as required by R2.

[13] Further information on this violation is contained in the Disposition Document included as Attachment f.1.
[14] Further information on this violation is contained in the Disposition Document included as Attachment f.1.
[15] Further information on this violation is contained in the Disposition Document included as Attachment f.1.

The duration of the CIP-009-1 R1 and R2 violations was from July 1, 2008, the date the Standard became mandatory and enforceable for Table 1 entities, through August 29, 2008, the date URE completed its Mitigation Plan.

SERC concluded that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE is a small Balancing Authority with a low estimated summer peak and its Control Center cyber assets had only one external communications link, which was with its Reliability Coordinator.

PRC-005-1 R1 - OVERVIEW[16]
During the Audit, SERC determined that URE, as a Transmission Owner, did not address station batteries, DC control circuitry, voltage and current sensing devices or associated communication systems in its Protection System maintenance and testing program. In addition, URE's procedure did not identify the basis for relay testing.

The duration of the PRC-005-1 R1 violation was from June 18, 2007, the date the Reliability Standard became mandatory and enforceable, through October 21, 2008, when URE completed its Mitigation Plan.

SERC concluded that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE was conducting maintenance and testing as required by R2.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[17]

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,[18] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on June 10, 2010. The NERC BOTCC approved the Settlement Agreement, including SERC's assessment of a sixteen thousand dollar ($16,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. the violations constituted URE's first occurrence of violations of the subject NERC Reliability Standards;

[16] Further information on this violation is contained in the Disposition Document included as Attachment f.3.
[17] *See* 18 C.F.R § 39.7(d)(4).
[18] *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). *See also North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

2. Although URE submitted Self-Report forms for thirteen (13) of the violations at issue, the violations were not considered self-reported violations because URE's Self-Certification responses were due and submitted the following day;
3. SERC reported that URE was cooperative throughout the compliance enforcement process;
4. URE has a compliance program; although URE did not have a compliance program at the time of the violations, it implemented a compliance program as a part of the Settlement Agreement;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations did not pose a serious or substantial risk to the BPS, as discussed in the NOP; and
7. SERC 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 finds that the assessed penalty of sixteen thousand dollars ($16,000) is appropriate for the violation and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Attachments to be included as Part of this Notice of Penalty

The attachments to be included as part of this Notice of Penalty is the following documents:

a) Settlement Agreement by and between SERC and URE executed February 18, 2010, included as Attachment a;

b) URE's Self Certification for the CIP-002-9 dated July 10, 2008, included as Attachment b;

c) SERC's Screening Worksheet for the CIP-004-1 R2.1 violation dated July 14, 2009, included as Attachment c;

d) SERC's Screening Worksheet for the PRC-005-1 R1 violation dated September 17, 2008, included as Attachment e;

e) Disposition Document for Common Information, included as Attachment e;

   i. Disposition Document for CIP-002-1 R1, R2 and R3; CIP-003-1 R1, R2 and R3; CIP-007-1 R1; CIP-008-1 R1; and CIP-009-1 R1 and R2 included as Attachment e.1;

   ii. Disposition Document for CIP-004-1 R2, R3, R4 and R2.1 included as Attachment e.2;

   iii. Disposition Document for PRC-005-1 R1 included as Attachment e.3;

f) Record documents for CIP-002-1 R1 through R3 included as Attachment f:

   i. URE's Mitigation Plan #MIT-08-1111 for the CIP-002-1 R1, R2 and R3 violations dated August 15, 2008;

   ii. URE's Certification of Completion for the Mitigation Plan addressing the CIP-002-1 R1, R2 and R3 violations dated September 5, 2008;

   iii. SERC's Verification of Completion for the Mitigation Plan addressing the CIP-002-1 R1, R2 and R3 violations dated December 15, 2008;

g) Record documents for CIP-003-1 R1 through R3 included as Attachment g:

   i. URE's Mitigation Plan #MIT-08-1112 for the CIP-003-1 R1, R2 and R3 violations dated August 15, 2008;

   ii. URE's Certification of Completion for the Mitigation Plan addressing the CIP-003-1 R1, R2 and R3 violations dated October 20, 2008;

   iii. SERC's Verification of Completion for the Mitigation Plan addressing the CIP-003-1 R1, R2 and R3 violations dated December 15, 2008;

h) Record documents for CIP-004-1 R2 through R4 included as Attachment h:

   i. URE's Mitigation Plan #MIT-08-1113 for the CIP-004-1 R2, R3 and R4 violations dated September 5, 2008;

   ii. URE's Certification of Completion for the Mitigation Plan addressing the CIP-004-1 R2, R3 and R4 violations dated October 20, 2008;

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

iii. SERC's Verification of Completion for the CIP-004-1 R2, R3 and R4 violations dated December 15, 2008;

i) Record documents for CIP-004-1 R2.1 included as Attachment i:

i. URE's Mitigation Plan #MIT-09-2009 for the CIP-004-1 R2.1 violation dated September 3, 2009;

ii. URE's Certification of Completion for the Mitigation Plan addressing the CIP-004-1 R2.1 violation dated September 3, 2009;

iii. SERC's Verification of Completion for the CIP-004-1 R2.1 violation dated October 9, 2009;

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

i. URE's Mitigation Plan #MIT-08-1114 for the CIP-007-1 R1 violations dated September 5, 2008;

ii. URE's Certification of Completion for the Mitigation Plan addressing the CIP-007-1 R1 violations dated October 20, 2008;

iii. SERC's Verification of Completion for the Mitigation Plan addressing the CIP-007-1 R1 violations dated December 15, 2008;

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

i. URE's Mitigation Plan #MIT-08-1115 for the CIP-008-1 R1 violations dated August 15, 2008;

ii. URE's Certification of Completion for the Mitigation Plan addressing the CIP-008-1 R1 violations dated December 23, 2008;

iii. SERC's Verification of Completion for the CIP-008-1 R1 violations dated December 24, 2008;

l) Record documents for CIP-009-1 R1 and R2 included as Attachment l:

i. URE's Mitigation Plan #MIT-08-1116 for the CIP-009-1 R1 and R2 violations dated August 15, 2008;

ii. URE's Certification of Completion for the Mitigation Plan addressing the CIP-009-1 R1 and R2 violations dated September 5, 2008;

iii. SERC's Verification of Completion for the CIP-009-1 R1 and R2 violations dated December 15, 2008;

m) Record documents for PRC-005-1 R1 included as Attachment m

i. URE's Mitigation Plan #MIT-07-1230 dated September 22, 2008;

ii. URE's Certification of Completion for the PRC-005-1 R1 violation dated October 21, 2008; and

iii. SERC's Verification of Completion for the PRC-005-1 R1 violation dated October 22, 2008.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

A Form of Notice Suitable for Publication[19]

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

[19] *See* 18 C.F.R § 39.7(d)(6).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Notices and Communications

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

Gerald W. Cauley* President and Chief Executive Officer David N. Cook* Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609)452-8060 (609) 452-9550 – facsimile gerry.cauley@nerc.net david.cook@nerc.net Kenneth B. Keels, Jr.* Director of Compliance Andrea Koch* Manager of Compliance Enforcement SERC Reliability Corporation 2815 Coliseum Centre Drive Charlotte, NC 28217 (704) 940-8214 (704) 357-7914 – facsimile kkeels@serc1.org akoch@serc1.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Rebecca J. Michael* Assistant General Counsel V. 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 R. Scott Henry* President and CEO SERC Reliability Corporation 2815 Coliseum Centre Drive Charlotte, NC 28217 (704) 940-8202 (704) 357-7914 – facsimile shenry@serc1.org Marisa A. Sifontes* General Counsel Jacqueline E. Carmody*Legal Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7775 (704) 357-7914 – facsimile msifontes@serc1.org jcarmody@serc1.org

Conclusion

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
gerry.cauley@nerc.net
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
V. 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
SERC Reliability Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment f

Disposition Document for Common Information

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS

June 10, 2010

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

REGIONAL ENTITY
SERC Reliability Corporation (SERC)

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 **$16,000** FOR **FIFTEEN (15)** VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST ANY CONFIRMED OR SETTLED VIOLATIONS AND STATUS

[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.

ADDITIONAL COMMENTS

PRIOR 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 ☐
EXPLAIN

At the time of the violations, URE had no formal compliance program. As a part of the Settlement Agreement, URE implemented the following compliance process:

1. **Document its compliance program, indicating the levels of supervision, including a description of what constitutes sufficient resources to comply with the applicable NERC Reliability Standards;**
2. **Document how URE maintains and tracks all compliance activities and requirements;**
3. **Document and implement a compliance training or awareness program for its employees;**
4. **Document how URE will maintain compliance if a key compliance position is vacated or unavailable;**
5. **Document how URE is making compliance with the approved standards included in the roles and responsibilities of its employees; and**

6. **Attend on a yearly basis a SERC compliance seminar or other forum.**

The completion of this implementation was verified by SERC during the Spot Check.

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

See above.

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

YES ☐ NO ☒
IF YES, EXPLAIN

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

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

(9) ADDITIONAL SUPPORT FOR ASSESSED PENALTY OR SANCTION

OTHER RELEVANT INFORMATION:

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

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **12/12/2008** OR N/A ☐

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

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

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

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-002-1 R1, R2 and R3; CIP-003-1 R1, R2 and R3; CIP-007-1 R1; CIP-008-1 R1; and CIP-009-1 R1 and R2

DISPOSITION OF VIOLATION

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
SERC200800170	**08-064**
SERC200800171	**08-065**
SERC200800172	**08-066**
SERC200800173	**08-067**
SERC200800174	**08-068**
SERC200800175	**08-069**
SERC200800179	**08-073**
SERC200800180	**08-074**
SERC200800181	**08-075**
SERC200800182	**08-076**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-002-1	**1**	**Not specified**	**Medium**	**Severe**
CIP-002-1	**2**	**Not specified**	**High**	**Severe**
CIP-002-1	**3**	**Not specified**	**High**[1]	**Severe**
CIP-003-1	**1**	**Not specified**	**Medium**	**Severe**
CIP-003-1	**2**	**Not specified**	**Medium**	**Severe**
CIP-003-1	**3**	**Not specified**	**Lower**	**Severe**
CIP-007-1	**1**	**Not specified**	**Medium**[2]	**Severe**
CIP-008-1	**1**	**Not specified**	**Lower**	**Severe**
CIP-009-1	**1**	**Not specified**	**Medium**	**Severe**
CIP-009-1	**2**	**Not specified**	**Lower**	**Severe**

VIOLATION APPLIES TO THE FOLLOWING FUNCTIONS:

BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
X												X		

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.

[1] CIP-002-1 R3 has a "Medium" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF.
[2] CIP-007-1 R1 has a "Medium" VRF; R1.1, R1.2 and R1.3 each have a "Lower" VRF.

These Critical Assets are to be identified through the application of a risk-based assessment."

CIP-002-1 Requirement (R) 1, R2 and R3 provide:

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.**
- **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.**

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

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the

[3] Within the text of the Reliability Standards, "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.

operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- **R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,**
- **R3.2. The Cyber Asset uses a routable protocol within a control center; or**
- **R3.3. The Cyber Asset is dial-up accessible.**

The purpose statement of CIP-003-1 provides: "Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. …"

CIP-003-1 R1, R2, and R3 provide:

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

R2. Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

- **R2.1. The senior manager shall be identified by name, title, business phone, business address, and date of designation.**
- **R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.**
- **R2.3. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.**

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

- **R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).**
- **R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.**
- **R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.**

The purpose statement of CIP-007-1 provides: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s) …."

CIP-007-1 R1 provides:

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.**
- **R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.**
- **R1.3. The Responsible Entity shall document test results.**

The purpose statement of CIP-008-1 provides: "Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets…."

CIP-008-1 R1 provides:

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:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.
R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.
R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.
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.

The purpose statement of CIP-009-1 provides: "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...."

CIP-009-1 R1 and R2 provide:

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:
R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).
R1.2. Define the roles and responsibilities of responders.
R2. 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 DESCRIPTION

In July 2007, Unidentified Registered Entity (URE) had self-certified that it was "Substantially Compliant" with the required CIP Standards and Requirements. In December 2007, URE's Director in charge of a department left the company. Little to no work had taken place on CIP compliance since that time as a consequence of a low priority being given to it by the remaining staff. A new director was scheduled to start at the end of July 2008.

On June 30, 2008, after being notified of an upcoming self-certification, URE submitted six (6) self-report forms which indicated that it had not taken the necessary steps to reach compliance with NERC Reliability Standards CIP-002-1 Requirement (R) 1, R2 and R3; CIP-003-1 R1, R2 and R3; CIP-004-1 R2, R3 and R4,[4] CIP-007-1 R1; CIP-008-1 R1; and CIP-009-1 R1 and R2. On July 10, 2008, URE submitted self-certifications for the same Standards, again indicating that it was not compliant.[5]

For CIP-002-1, URE did not have a risk-based methodology to identify critical assets as required by R1 and therefore, did not have a list of Critical Assets as required by R2 and did not have a list of associated Critical Cyber Assets as required by R3.

For CIP-003-1, URE did not have a cyber security policy as required by R1, did not assign a senior Manager as required by R2 and did not document exceptions as required by R3.

Because URE did not identify any Critical Cyber Assets, URE was not in compliance with CIP-007-1 R1, CIP-008-1 R1, and CIP-009-1 R1 and R2. Specifically:

- **for CIP-007-1 R1, URE did not create, implement and maintain test procedures to ensure existing cyber security controls are still in place after changes to cyber assets;**
- **for CIP-008-1 R1, URE did not develop and maintain a Cyber Security Incident response plan; and**
- **for CIP-009-1, URE did not create and annually review recovery plans for Critical Cyber Assets as required by R1 and therefore, did not exercise its recovery plans as required by R2.**

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

SERC determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because URE is a small Balancing Authority with a low estimated summer peak and its Control Center cyber assets had only one external communications link, which was with its Reliability Coordinator.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT	☐
SELF-CERTIFICATION	☒
COMPLIANCE AUDIT	☐

[4] The CIP-004-1 R2, R3 and R4 violations are addressed in attachment b.2.
[5] In July 2007, URE had self-certified that it was substantially compliant with the CIP Standards as required.

COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK	☐
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

URE Self-Reported the violations on June 30, 2008, after being notified of the upcoming Self-Certification and one day before its Self-Certification responses were due.

DURATION DATE(S)

- **CIP-002-1 R1, R2 and R3: 7/1/2008 (mandatory and enforceable date for Table 1[6] entities) through 8/29/2008 (Mitigation Plan completion)**
- **CIP-003-1 R1: 7/1/2008 (mandatory and enforceable date for Table 1 entities) through 9/12/2008 (when URE mitigated the violation by documenting and implementing its cyber security policy)**
- **CIP-003-1 R2: 7/1/2008 (mandatory and enforceable date for Table 1 entities) through 8/22/2008 (when URE mitigated the violation by identifying a senior manager)**
- **CIP-003-1 R3: 7/1/2008 (mandatory and enforceable date for Table 1 entities) through 9/26/2008 (when URE mitigated the violation by identifying any exceptions to its cyber security policy)**
- **CIP-007-1 R1: 7/1/2008 (mandatory and enforceable date for Table 1 entities) through 10/10/2008 (Mitigation Plan completion)**
- **CIP-008-1 R1: 7/1/2008 (mandatory and enforceable date for Table 1 entities) through 12/23/2008 (Mitigation Plan completion)**
- **CIP-009-1 R1 and R2: 7/1/2008 (mandatory and enforceable date for Table 1 entities) through 8/29/2008 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **6/30/2008 (See above comment in Method of Discovery)**

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	☒

[6] *See Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1*.

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **See chart below**
DATE SUBMITTED TO REGIONAL ENTITY **See chart below**
DATE ACCEPTED BY REGIONAL ENTITY **See chart below**
DATE APPROVED BY NERC **See chart below**
DATE PROVIDED TO FERC **See chart below**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **See chart below**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **See chart below**

DATE OF CERTIFICATION LETTER **See chart below**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **See 'Actual Completion' dates in chart below**

DATE OF VERIFICATION LETTER **See chart below**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **See 'Actual Completion' dates in chart below**

	CIP-002-1 R1, R2, R3	**CIP-003-1 R1, R2, R3**	**CIP-007-1 R1**	**CIP-008-1 R1**	**CIP-009-1 R1, R2**
MP #	MIT-08-1111	MIT-08-1112	MIT-08-1114	MIT-08-1115	MIT-08-1116
Submitted to SERC	8/15/2008	8/15/2008	9/5/2008	9/5/2008	8/15/2008
Accepted by SERC	10/22/2008	10/22/2008	10/22/2008	10/22/2008	10/22/2008
Approved by NERC	11/10/2008	11/10/2008	11/10/2008	11/10/2008	11/10/2008
Provided to FERC	11/10/2008	11/10/2008	11/10/2008	11/10/2008	11/10/2008
Expected Completion	9/5/2008	9/26/2008	10/10/2008	1/2/2009	9/26/2008
Actual Completion	8/29/2008	9/26/2008	10/10/2008	12/23/2008	8/29/2008
Certification Letter	9/5/2008	10/20/2008	10/20/2008	12/23/2008	9/5/2008
Verification	12/15/2008	12/15/2008	12/15/2008	12/24/2008	12/15/2008

Letter					

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

For CIP-002-1 R1, R2 and R3, URE:

- **identified and documented a risk-based assessment methodology to identify its critical assets to comply with R1;**
- **developed a list of critical assets using its risk-based assessment methodology to comply with R2; and**
- **developed a list of critical cyber assets essential to the operation of its critical assets to comply with R3.**

For CIP-003-1 R1, R2 and R3, URE:

- **documented and implemented a cyber security policy that represented management's commitment and ability to secure its Critical Cyber Assets to comply with R1;**
- **assigned a senior manager with overall responsibility for leading URE's implementation and adherence to CIP-002 through CIP-009 to comply with R2; and**
- **documented and authorized any exceptions to its cyber security policy to comply with R3.**

For CIP-007-1 R1, URE:

- **documented its cyber security controls, the last time cyber assets were added to the electronic security perimeter and the last time a significant software change was made to a Critical Cyber Asset; and**
- **developed a policy that addressed adding or changing existing cyber assets.**

For CIP-008-1 R1, URE:

- **identified its Critical Cyber Assets to comply with R1; and**
- **finalized its incident response plan.**

For CIP-009-1 R1 and R2, URE:

- **created and reviewed recovery plans for Critical Cyber Assets to comply with R1; and**
- **exercised its recovery plan. URE's plan requires it to continue to exercise its plan on a quarterly basis to comply with R2.**

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)

For compliance with CIP-002-1 R1, R2 and R3, SERC reviewed:

- **URE's risk-based assessment methodology; and**
- **URE's Critical Asset and Critical Cyber Asset lists .**

For compliance with CIP-003-1 R1, R2 and R3, SERC reviewed:

- **URE's security policy;**
- **URE's delegation of responsibility statement;**
- **URE's Declaration of Senior Manager; and**
- **URE's list of exceptions to its policy statement.**

For compliance with CIP-007-1 R1, SERC reviewed:

- **URE's software and hardware testing policy; and**
- **URE's current cyber security controls.**

For compliance with CIP-008-1 R1, SERC reviewed:

- **URE's Critical Asset and Critical Cyber Asset lists; and**
- **URE's incident response plan.**

For compliance with CIP-009-1 R1 and R2, SERC reviewed:

- **URE's cyber recovery plan.**

EXHIBITS (SEE ATTACHMENTS TO NOTICE OF PENALTY):

SOURCE DOCUMENTS
URE's Self Certification for the CIP-002-009 violations dated July 10, 2008

MITIGATION PLANS
URE's Mitigation Plan designated as MIT-08-1111 for the CIP-002-1 R1, R2 and R3 violations dated August 15, 2008

URE's Mitigation Plan designated as MIT-08-1112 for the CIP-003-1 R1, R2 and R3 violations dated August 15, 2008

URE's Mitigation Plan designated as MIT-08-1114 for the CIP-007-1 R1 violations dated September 5, 2008

URE's Mitigation Plan designated as MIT-08-1115 for the CIP-008-1 R1 violations dated September 5, 2008

URE's Mitigation Plan designated as MIT-08-1116 for the CIP-009-1 R1 and R2 violations dated August 15, 2008

CERTIFICATIONS BY REGISTERED ENTITY

URE's Certification of Completion for the Mitigation Plan addressing the CIP-002-1 R1, R2 and R3 violations dated September 5, 2008

URE's Certification of Completion for the Mitigation Plan addressing the CIP-003-1 R1, R2 and R3 violations dated October 20, 2008

URE's Certification of Completion for the Mitigation Plan addressing the CIP-007-1 R1 violations dated October 20, 2008

URE's Certification of Completion for the Mitigation Plan addressing the CIP-008-1 R1 violations dated December 23, 2008

URE's Certification of Completion for the Mitigation Plan addressing the CIP-009-1 R1 and R2 violations dated September 5, 2008

VERIFICATION BY REGIONAL ENTITY

SERC's Verification of Completion for the Mitigation Plan addressing the CIP-002-1 R1, R2 and R3 violations dated December 15, 2008

SERC's Verification of Completion for the Mitigation Plan addressing the CIP-003-1 R1, R2 and R3 violations dated December 15, 2008

SERC's Verification of Completion for the Mitigation Plan addressing the CIP-007-1 R1 violations dated December 15, 2008

SERC's Verification of Completion for the Mitigation Plan addressing the CIP-008-1 R1 violations dated December 24, 2008

SERC's Verification of Completion for the Mitigation Plan addressing the CIP-009-1 R1 and R2 violations dated December 15, 2008

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

DISPOSITION OF VIOLATION

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
SERC200800176	**08-070**
SERC200800177	**08-071**
SERC200800178	**08-072**
SERC200900291	**09-050**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**2**	**Not specified**	**Medium**	**Severe**
CIP-004-1	**3**	**Not Specified**	**Medium**	**Severe**
CIP-004-1	**4**	**Not Specified**	**Medium**	**Severe**
CIP-004-1	**2**	**2.1**	**Medium**	**Lower**

VIOLATION APPLIES TO THE FOLLOWING FUNCTIONS:

BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
X												X		

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.**

CIP-004-1 Requirement (R) 2, R3 and R4 provide:

> **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.

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 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

In July 2007, Unidentified Registered Entity (URE) had self-certified that it was "Substantially Compliant" with the required CIP Standards and Requirements. In December 2007, URE's Director in charge of a department left the company. Little to no work had taken place on CIP compliance since that time as a consequence of a low priority being given to it by the remaining staff. A new director was scheduled to start at the end of July 2008.

On June 30, 2008, after being notified of an upcoming self-certification, URE submitted a self-report form, which indicated that it had not taken the necessary steps to reach compliance with NERC Reliability Standard CIP-004-1 Requirement (R) 2, R3 and R4. On July 1, 2008, URE submitted a self-certification for the same Standard, again indicating that it was not compliant.[1]

Specifically, URE did not establish, maintain and document a cyber security training program as required by R2; implement and document a personnel risk assessment program as required by R3; and maintain list(s) of personnel with Critical Cyber Assets access rights as required by R4.

On August 15, 2008, URE submitted a Mitigation Plan to mitigate its noncompliance with CIP-004-1 R2, R3 and R4. URE completed this Mitigation Plan on October 3, 2008 and SERC verified the completion on December 15, 2008.

In discussions held on December 8, 2008, URE and SERC agreed that SERC would conduct an on-site Spot Check of URE compliance with the CIP Standards, which was conducted from July 13, 2009, through July 14, 2009. SERC determined that URE was in compliance with all of the CIP requirements and sub-requirements subject to the Spot Check, with the exception of CIP-004-1 R2.1. SERC found that URE had not trained its existing staff within ninety (90) days of granting access to Critical Cyber Assets or within ninety (90) days of July 1, 2008, the effective date of the Standard.

SERC found that the fact that URE had not trained its existing staff was an oversight in the start-up of URE's CIP compliance program. While URE trained its

[1] In July 2007, URE had self-certified that it was substantially compliant with the CIP Standards as required.

new employees within ninety (90) days of access to Critical Cyber Assets, it did not recognize that it needed to train its existing employees, because it thought the existing staff was grandfathered in and did not need to be trained.[2] Instead, URE scheduled its existing employees for training in accordance with its newly established annual training schedule, which first took place on May 12, 2009. Therefore, SERC determined that URE was compliant at the time of the Spot Check, but URE had a gap in compliance from July 1, 2008 through May 12, 2009.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

SERC determined that the 2008 violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because URE is a small Balancing Authority with a low estimated summer peak and its Control Center Cyber Assets had only one external communications link, with was with its Reliability Coordinator.

SERC determined that the 2009 violation of CIP-004-1 R2.1 for the gap in training did not pose a serious or substantial risk to the reliability of the BPS because the employees that did not receive the timely training were existing employees that had experience with URE's Critical Cyber Assets.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT	☐
SELF-CERTIFICATION (R2, R3, R4)	☒
COMPLIANCE AUDIT	☐
COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK (R2.1)	☒
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

URE Self-Reported the violation of CIP-004-1 R2, R3 and R4 on June 30, 2008, after being notified of the upcoming Self-Certification and one day before its Self-Certification responses were due.

[2] The Mitigation Plan for the first violation of CIP-004-1 R2 focused on developing a training program, which SERC verified; however, SERC did not review training records to confirm that all employees received the required training. At the Spot Check, SERC reviewed training records to verify that URE had implemented its program and was in compliance with CIP-004-1 R2. Therefore, URE's misunderstanding of the Standard and failure to train its existing employees within ninety (90) days of the effective date of the Standard was not discovered until the Spot Check.

SERC discovered the gap in compliance with CIP-004-1 R2.1 during the July 2009 Spot Check.

DURATION DATE(S)

- **CIP-004-1 R2: 7/1/2008 (mandatory and enforceable date for Table 1[3] entities) through 10/3/2008 (when URE completed its Mitigation Plan)**
- **CIP-004-1 R3: 7/1/2008 (mandatory and enforceable date for Table 1 entities) through 9/26/2008 (when URE completed its Personnel Risk Assessments)**
- **CIP-004-1 R4: 7/1/2008 (mandatory and enforceable date for Table 1 entities) through 8/29/2008 (when URE completed its list of personnel with access to Critical Cyber Assets)**
- **CIP-004-1 R2.1: 7/1/2008 (mandatory and enforceable date for Table 1 entities) through 5/12/2009 (when URE completed its training for existing personnel)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

CIP-004-1 R2, R3 and R4: 6/30/08 (See above comment in Method of Discovery)

CIP-004-1 R2.1: 7/13/2009 through 7/14/2009

IS THE VIOLATION STILL OCCURRING
YES ☐ NO ☒
IF YES, EXPLAIN
See comment above in Method of Discovery

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. **See chart below**
DATE SUBMITTED TO REGIONAL ENTITY **See chart below**
DATE ACCEPTED BY REGIONAL ENTITY **See chart below**
DATE APPROVED BY NERC **See chart below**
DATE PROVIDED TO FERC **See chart below**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

[3] According to the *Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1*.

EXPECTED COMPLETION DATE **See chart below**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **See chart below**

DATE OF CERTIFICATION LETTER **See chart below**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **See 'Actual Completion' dates in chart below**

DATE OF VERIFICATION LETTER **See chart below**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **See 'Actual Completion' dates in chart below**

	CIP-004-1 R2, R3, R4	**CIP-004-1 R2.1**
MP #	MIT-08-1113	MIT-09-2009
Submitted to SERC	8/15/2008	9/3/2009
Accepted by SERC	10/22/2008	9/25/2009
Approved by NERC	11/10/2008	9/28/2009
Provided to FERC	11/10/2008	9/28/2009
Expected Completion	10/3/2008	Submitted as complete as of 5/12/2009
Verified Actual Completion	10/3/2008	5/12/2009
Certification Letter	10/20/2008	9/3/2009
Verification Letter	12/15/2008	10/9/2009

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

For CIP-004-1 R2, R3 and R4, URE:

- **URE established, maintained, and documented an annual cyber security training program to comply with R2;**
- **URE documented a personnel risk assessment program to comply with R3; and**
- **URE maintained a list of personnel with authorized cyber or authorized unescorted physical access to critical cyber assets to comply with R4.**

For CIP-004-1 R2.1, URE:

- **Trained its existing personnel during its annual training on May 12, 2009. This action corrected URE's neglect to train its existing personnel after the Standard became mandatory and enforceable.**

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)

For compliance with CIP-004-1 R2, R3 and R4 SERC reviewed:

- **URE documented training program;**
- **URE Personnel Risk Assess Program *(Background Checks)*; and**
- **URE personnel access lists.**

For compliance with CIP-004-1 R2.1 SERC reviewed records verifying compliance with R2.1 during a CIP Spot-check.

EXHIBITS (SEE ATTACHMENTS TO NOTICE OF PENALTY):

SOURCE DOCUMENTS
URE's Self Certification for the CIP-002-009 violations dated July 10, 2008

SERC's Screening Worksheet for the CIP-004-1 R2.1 violation dated July 14, 2009
MITIGATION PLANS

URE's Mitigation Plan for the CIP-004-1 R2, R3 and R4 violations dated August 15, 2008

URE's Mitigation Plan for the CIP-004-1 R2.1 violation dated September 3, 2009

CERTIFICATIONS BY REGISTERED ENTITY

URE's Certification of Completion for the Mitigation Plan addressing the CIP-004-1 R2, R3 and R4 violations dated October 20, 2008

URE's Certification of Completion for the Mitigation Plan addressing the CIP-004-1 R2.1 violation dated September 3, 2009

VERIFICATION BY REGIONAL ENTITY

SERC's Verification of Completion for the CIP-004-1 R2, R3 and R4 violations dated December 15, 2008

SERC's Verification of Completion for the CIP-004-1 R2.1 violation dated October 9, 2009

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for PRC-005-1 R1

DISPOSITION OF VIOLATION

NERC TRACKING NO. **SERC200800200**

REGIONAL ENTITY TRACKING NO. **08-116**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
PRC-005-1	**1**	**Not specified**	**High**[1]	**Severe**

VIOLATION APPLIES TO THE FOLLOWING FUNCTIONS:

BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
											X			

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

The purpose of PRC-005-1 is "[t]o ensure all transmission and generation Protection Systems affecting the reliability of the Bulk Electric System (BES) are maintained and tested."

PRC-005-1 R1 requires that:

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

During a compliance audit (Audit), SERC Compliance Audit Staff (SERC Staff) discovered that Unidentified Registered Entity's (URE) procedure provided to demonstrate compliance with NERC Reliability Standard PRC-005-1 R1 did not address each of the components of its transmission Protection System, as required by the standard. Specifically, URE's Protection System Maintenance and Testing Program document did not address station batteries, DC control circuitry, voltage

[1] When NERC filed VRFs for PRC-005-1, NERC originally assigned a "Medium" VRF to PRC-005-1 R1. In the Commission's May 18, 2007 Order on Violation Risk Factors, the Commission approved the VRF as filed but directed modifications. On June 1, 2007, NERC filed a modified "High" VRF for PRC-005 R1 for approval. On August 6, 2007, the Commission issued an Order approving the modified VRF. Therefore, the "Medium" VRF was in effect from June 18, 2007 until August 6, 2007 and the "High" VRF has been in effect since August 6, 2007.

and current sensing devices or associated communication systems in its program documentation. In addition, URE's procedure did not identify the basis for relay testing.

URE promptly provided additional evidence in the form of maintenance records to substantiate that it was performing all required maintenance and testing of its Protection System. Upon review of the evidence that URE provided, SERC Staff found that URE was performing the required maintenance on all of the elements of its transmission Protection System, as required in NERC Reliability Standard PRC-005-1 R2 and that URE was in compliance with R2 of the Standard.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

SERC determined that the violation did not pose a serious or substantial risk to the reliability of the BPS because URE was conducting maintenance and testing as required by R2.

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) **June 18, 2007, the date the Reliability Standard became mandatory and enforceable, through October 21, 2008, when URE completed its Mitigation Plan**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **9/17/2008**

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-07-1230**
DATE SUBMITTED TO REGIONAL ENTITY **9/22/2008**
DATE ACCEPTED BY REGIONAL ENTITY **11/20/2008**
DATE APPROVED BY NERC **12/18/2008**
DATE PROVIDED TO FERC **12/18/2008**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **10/17/2008**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **10/21/2008**

DATE OF CERTIFICATION LETTER **10/21/2008**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **10/21/2008**

DATE OF VERIFICATION LETTER **10/22/2008**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **10/21/2008**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

To comply with PRC-005-1 R1, URE:

- **Modified its plan to include all applicable Protection System devices in its program document;**
- **Documented its testing and maintenance summaries and intervals; and**
- **added the additional Protection System devices to its tracking database.**

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)

SERC reviewed:

- **URE's Protection System Maintenance Plan which included a description of the maintenance and testing to be performed, maintenance intervals, and their bases for all elements of a Protection System as defined in the NERC Glossary of Terms.**

EXHIBITS (SEE ATTACHMENTS TO NOTICE OF PENALTY):

SOURCE DOCUMENT
SERC's Screening Worksheet dated September 17, 2008

MITIGATION PLAN
URE's Mitigation Plan dated September 22, 2008

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Completion dated October 21, 2008

VERIFICATION BY REGIONAL ENTITY
SERC's Verification of Completion dated October 22, 2008