PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

June 29, 2011

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

Re: NERC Abbreviated Notice of Penalty regarding Unidentified Registered Entity 1, Unidentified Registered Entity 2 and Unidentified Registered Entity 3, 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 1 (URE-1), Unidentified Registered Entity 2 (URE-2) and Unidentified Registered Entity 3 (URE-3), and the parent company (URE Subsidiaries), 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 Northeast Power Coordinating Council, Inc. (NPCC) and URE Subsidiaries have entered into a Settlement Agreement to resolve all outstanding issues arising from NPCC's determination and findings of the violations of CIP-004-1 R2, CIP-004-1 R3, CIP-004-1 R4 (ten occurrences), CIP-004-2 R4 (two occurrences), CIP-006-1 R2 (six occurrences), and CIP-006-2 R4. According to the Settlement Agreement, URE Subsidiaries neither admit nor deny the violations, but have agreed to the assessed penalty of

[1] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.
[2] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (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

eighty thousand dollars ($80,000), 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 NPCC200900088, NPCC200900089, NPCC200900090, NPCC200900091, NPCC200900092, NPCC200900096, NPCC200900115, NPCC201000147, NPCC201000148, NPCC201000149, NPCC201000150, NPCC201000151, NPCC201000152, NPCC200900103, NPCC200900104, NPCC200900105, NPCC200900114, NPCC201000146, NPCC201000156, NPCC200900181, and NPCC200900182 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This NOP incorporates the findings and justifications set forth in the Settlement Agreement executed on June 14, 2011, by and between NPCC and URE Subsidiaries. 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[3]	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
NOC-859	NPCC200900088	CIP-004-1	4.2	Medium[4]	7/1/09-7/20/09	80,000
	NPCC200900089	CIP-004-1	4.2	Medium	7/1/09-7/21/09	
	NPCC200900090	CIP-004-1	4.2	Medium	7/9/09-7/21/09	
	NPCC200900091	CIP-004-1	4.2	Medium	7/20/19-7/21/09	
	NPCC200900092	CIP-006-1	2, 2.3	Medium	7/27/09-7/27/09	
	NPCC200900096	CIP-006-1	2, 2.1	Medium	8/12/09-8/12/09	
	NPCC200900115	CIP-004-1	4.2	Medium	10/11/09-10/21/09	

[3] URE-1 had the following violations; NPCC200900088, 089, 090, 091, 092, 096, 115, NPCC201000147, 148, 149, 150, 151, 152. URE-2 had the following violations; NPCC200900103, 104, 105, 114, NPCC201000146, 156. URE-3 had the following violations; NPCC201000181 and 182.
[4] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF.

	NPCC201000147	CIP-004-1	2.1	Medium[5]	7/1/09-2/18/10	
	NPCC201000148	CIP-004-1	3	Medium[6]	7/1/09-9/30/09	
	NPCC201000149	CIP-004-1	4.1	Lower	10/1/09-5/15/09	
	NPCC201000150	CIP-004-1	4.2	Medium	10/8/09-10/13/09	
	NPCC201000151	CIP-004-1	4.2	Medium	7/1/09-9/8/09	
	NPCC201000152	CIP-006-1	2	Medium	2/20/10-2/22/10	
	NPCC200900103	CIP-004-1	4.2	Medium	7/27/09-8/20/10	
	NPCC200900104	CIP-006-1	2	Medium	8/19/09-11/9/09	
	NPCC200900105	CIP-006-1	2	Medium	8/19/09-11/9/09	
	NPCC200900114	CIP-006-1	2	Medium	12/2/09-12/4/09	
	NPCC201000146	CIP-004-1	4.1	Lower	10/1/09-5/30/10	
	NPCC201000156	CIP-006-2	4	Medium	5/8/10-5/28/10	
	NPCC200900181	CIP-004-2	4, 4.2	Medium	6/8/10-6/14/10	
	NPCC200900182	CIP-004-2	4, 4.2	Medium	7/7/10-8/5/10	

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

URE-1 Violations:

NPCC200900088 – CIP-004-1 R4.2 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 did not disable (revoke), within seven days, physical access to Critical Cyber Assets (CCAs) for a substation employee who was transferred to a new position.

[5] When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.
[6] CIP-004-1 R3 has a "Medium" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF.

NPCC200900089 – CIP-004-1 R4.2 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 did not disable (revoke), within seven days, physical access to CCAs for a Control Center employee who was transferred to a new position.

NPCC200900090 – CIP-004-1 R4.2 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 did not disable (revoke), within 24 hours, physical access to CCAs for a Control Center employee who was terminated for cause.

NPCC200900091 – CIP-004-1 R4.2 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 did not disable (revoke), within seven days, physical access to CCAs for a Control Center employee who was transferred to a new position.

NPCC200900092 – CIP-006-1 R2, R2.3 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 had a contractor, without authorized physical access to critical cyber assets, access its facility by being provided an access route that was not in conformance with the security perimeter that was installed.

NPCC200900096 – CIP-006-1 R2, R2.1 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 had a key card reader installed on rooms housing CCAs, but did not disable a prior locking mechanism to prevent access to an unauthorized communications company employee who had previously been issued keys.

NPCC200900115 – CIP-004-1 R4.2 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 did not disable (revoke), within seven days, physical access to CCAs for a substation employee who was transferred to a new position.

NPCC201000147 – CIP-004-1 R2.1 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 did not provide the required CIP training within ninety days of authorization for five employees with read-only access to the Energy Management System (EMS), a CCA.

NPCC201000148 – CIP-004-1 R3 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 did not have the required personnel risk assessment performed within thirty days of granting read-only access to the EMS, a CCA, for one employee.

NPCC201000149 – CIP-004-1 R4.1 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 had incomplete lists of personnel with authorized unescorted physical access to critical cyber assets along with their specific physical access rights.

NPCC201000150 – CIP-004-1 R4.2 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 did not disable (revoke), within seven days, physical access to CCAs for a substation employee who retired.

NPCC201000151 – CIP-004-1 R4.2 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 did not disable (revoke), within seven days, physical access to CCAs for a substation employee who was transferred to a new position.

NPCC201000152 – CIP-006-1 R2 - OVERVIEW
URE-1 submitted a self-report to NPCC for this violation. NPCC determined that URE-1 had a key card reader installed on rooms housing CCAs, but did not disable a prior locking mechanism to prevent access to three security guards escorting a contractor, who were not authorized for unescorted physical access to CCAs but who had previously been issued keys.

URE-2 Violations:

NPCC200900103 – CIP-004-1 R4.2 - OVERVIEW
URE-2 submitted a self-report to NPCC for this violation. NPCC determined that URE-2 failed to revoke, within seven days, the access rights of an employee who had transferred to a new position and no longer required physical access right to Critical Cyber Assets.

NPCC200900104 – CIP-006-1 R2 - OVERVIEW
URE-2 submitted a self-report to NPCC for this violation. NPCC determined that URE-2 had an employee use a key that previously had been provided, instead of the required card key, to access a substation control house physical security perimeter.

NPCC200900105 – CIP-006-1 R2 - OVERVIEW
URE-2 submitted a self-report to NPCC for this violation. NPCC determined that URE-2 had two employees use a key that previously had been provided, instead of the required card key, to access a substation control house physical security perimeter.

NPCC200900114 – CIP-006-1 R2 - OVERVIEW
URE-2 submitted a self-report to NPCC for this violation. NPCC determined that URE-2 had a contractor employee use a key that had previously been provided, instead of the required card key, to access a substation control house physical security perimeter.

NPCC200900146 – CIP-004-1 R4.1 - OVERVIEW
URE-2 submitted a self-report to NPCC for this violation. NPCC determined that URE-2 had an incomplete access list of personnel with authorized unescorted access to critical cyber assets along with specific physical access rights.

NPCC200900156 – CIP-006-2 R4 - OVERVIEW
URE-2 submitted a self-report to NPCC for this violation. NPCC determined that URE-2 had two occasions when unauthorized employees, through the use of a master key, gained access to a vacant control room containing a CCA, an EMS computer workstation.

URE-3 Violations:

NPCC200900181 – CIP-004-2 R4, R4.2 - OVERVIEW
URE-3 submitted a self-report to NPCC for this violation. NPCC determined that URE-3 did not revoke access within seven days after a contractor no longer required unescorted physical access to CCAs.

NPCC200900182 – CIP-004-2 R4, R4.2 - OVERVIEW
URE-3 submitted a self-report to NPCC for this violation. NPCC determined that URE-3 did not revoke access within seven days after a contractor employee retired and no longer required unescorted physical access to CCAs.

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

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines, the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on May 9, 2011. The NERC BOTCC approved the Settlement Agreement, including NPCC's assessment of an eighty thousand dollar ($80,000) financial penalty against URE Subsidiaries 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:[9]

[7] *See* 18 C.F.R. § 39.7(d)(4).
[8] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).
[9] NPCC considered URE Subsidiaries' compliance program a neutral factor in determining the penalty, as discussed in the Disposition Documents.

1. the violations constituted URE Subsidiaries' first violation of the subject NERC Reliability Standards;
2. URE Subsidiaries self-reported the violations;
3. NPCC reported that URE Subsidiaries were cooperative throughout the compliance enforcement process;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. NPCC determined that the violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), as discussed in the Disposition Documents; and
6. NPCC 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 eighty thousand dollars ($80,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

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

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

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

Attachments to be included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between NPCC and URE Subsidiaries executed June 14, 2011, included as Attachment a;
    i. Disposition of Violations for URE-1, included as Attachment A to the Settlement Agreement;
    ii. Disposition of Violations for URE-2, included as Attachment B to the Settlement Agreement; and
    iii. Disposition of Violations forURE-3, included as Attachment C to the Settlement Agreement.
b) Record Documents for URE-1's CIP-004-1 R4.2 Violations NPCC200900088, NPCC200900089, NPCC200900090, and NPCC200900091:
    i. URE-1's Self-Report for NPCC200900088, included as Attachment b-1;
    ii. URE-1's Self-Report for NPCC200900089, included as Attachment b-2;
    iii. URE-1's Self-Report for NPCC200900090, included as Attachment b-3;
    iv. URE-1's Self-Report for NPCC200900091, included as Attachment b-4;
    v. URE-1's Mitigation Plan MIT-09-2356, included as Attachment b-5;
    vi. URE-1's Certification of Mitigation Plan Completion, included as Attachment b-6; and
    vii. NPCC's Verification of Mitigation Plan Completion, included as Attachment b-7.
c) Record Documents for NPCC200900092:[10]
    i. URE-1's Self-Report, included as Attachment c-1;
    ii. URE-1's Mitigation Plan MIT-09-2357, included as Attachment c-2;
    iii. URE-1's Certification of Mitigation Plan Completion, included as Attachment c-3; and
    iv. NPCC's Verification of Mitigation Plan Completion, included as Attachment b-7.
d) Record Documents for NPCC200900096:
    i. URE-1's Self-Report, included as Attachment d-1;
    ii. URE-1's Mitigation Plan MIT-09-2358, included as Attachment d-2;
    iii. URE-1's Certification of Mitigation Plan Completion, included as Attachment d-3; and
    iv. NPCC's Verification of Mitigation Plan Completion, included as Attachment b-7.
e) Record Documents for NPCC200900115:
    i. URE-1's Self-Report, included as Attachment e-1;
    ii. URE-1's Mitigation Plan MIT-09-2399, included as Attachment e-2;

[10] The supporting documents for the CIP-006 R2 (NPCC200900092) violation also references violations of CIP-006 R3.2 (NPCC200900094) and CIP-006 R4.3 (NPCC200900095); NPCC dismissed these violations on March 22, 2010.

iii. URE-1's Certification of Mitigation Plan Completion, included as Attachment e-3; and
iv. NPCC's Verification of Mitigation Plan Completion, included as Attachment b-7.

f) Record Documents for NPCC201000147 and NPCC201000148:
i. URE-1's Self-Report for NPCC201000147, included as Attachment f-1;
ii. URE-1's Self-Report for NPCC201000148, included as Attachment f-2;
iii. URE-1's Mitigation Plan MIT-09-2603, included as Attachment f-3;
iv. URE-1's Certification of Mitigation Plan Completion for NPCC201000147, included as Attachment f-4;
v. URE-1's Certification of Mitigation Plan Completion for NPCC201000148, included as Attachment f-5; and
vi. NPCC's Verification of Mitigation Plan Completion, included as Attachment b-7.

g) Record Documents for NPCC201000149:
i. URE-1's Self-Report, included as Attachment g-1;
ii. URE-1's Mitigation Plan MIT-09-2579, included as Attachment g-2;
iii. URE-1's Certification of Mitigation Plan Completion, included as Attachment g-3; and
iv. NPCC's Verification of Mitigation Plan Completion, included as Attachment b-7.

h) Record Documents for NPCC201000150:
i. URE-1's Self-Report, included as Attachment h-1;
ii. URE-1's Mitigation Plan MIT-09-2580, included as Attachment h-2;
iii. URE-1's Certification of Mitigation Plan Completion, included as Attachment h-3; and
iv. NPCC's Verification of Mitigation Plan Completion, included as Attachment b-7.

i) Record Documents for NPCC201000151:
i. URE-1's Self-Report, included as Attachment i-1;
ii. URE-1's Mitigation Plan MIT-09-2581, included as Attachment i-2;
iii. URE-1's Certification of Mitigation Plan Completion, included as Attachment i-3; and
iv. NPCC's Verification of Mitigation Plan Completion, included as Attachment b-7.

j) Record Documents for NPCC201000152:
i. URE-1's Self-Report, included as Attachment j-1;
ii. URE-1's Mitigation Plan MIT-09-2582, included as Attachment j-2;
iii. URE-1's Certification of Mitigation Plan Completion, included as Attachment j-3; and
iv. NPCC's Verification of Mitigation Plan Completion, included as Attachment b-7.

k) Record Documents for NPCC200900103:
i. URE-2's Self-Report, included as Attachment k-1;
ii. URE-2's Mitigation Plan MIT-09-2359, included as Attachment k-2;

iii. URE-2's Certification of Mitigation Plan Completion, included as Attachment k-3; and
iv. NPCC's Verification of Mitigation Plan Completion, included as Attachment k-4.

l) Record Documents for NPCC200900104 and NPCC200900105:
i. URE-2's Self-Report for NPCC200900104, included as Attachment l-1;
ii. URE-2's Self-Report for NPCC200900105, included as Attachment l-2;
iii. URE-2's Mitigation Plan MIT-09-2360, included as Attachment l-3;
iv. URE-2's Certification of Mitigation Plan Completion, included as Attachment l-4; and
v. NPCC's Verification of Mitigation Plan Completion, included as Attachment k-4.

m) Record Documents for NPCC200900114:
i. URE-2's Self-Report, included as Attachment m-1;
ii. URE-2's Mitigation Plan MIT-09-2398, included as Attachment m-2;
iii. URE-2's Certification of Mitigation Plan Completion, included as Attachment m-3; and
iv. NPCC's Verification of Mitigation Plan Completion, included as Attachment k-4.

n) Record Documents for NPCC201000146:
i. URE-2's Self-Report, included as Attachment n-1;
ii. URE-2's Mitigation Plan MIT-09-2577 s, included as Attachment n-2;
iii. URE-2's Certification of Mitigation Plan Completion, included as Attachment n-3; and
iv. NPCC's Verification of Mitigation Plan Completion, included as Attachment k-4.

o) Record Documents for NPCC201000156:
i. URE-2's Self-Report, included as Attachment o-1;
ii. URE-2's Mitigation Plan MIT-10-2933, included as Attachment o-2;
iii. URE-2's Certification of Mitigation Plan Completion, included as Attachment o-3; and
iv. NPCC's Verification of Mitigation Plan Completion, included as Attachment k-4.

p) Record Documents for NPCC200900181 and NPCC200900182:
i. URE-3's Self-Report for NPCC200900181, included as Attachment p-1;
ii. URE-3's Self-Report for NPCC200900182, included as Attachment p-2;
iii. URE-3's Mitigation Plan MIT-10-3404, included as Attachment p-3;
iv. URE-3's Certification of Mitigation Plan Completion, included as Attachment p-4; and
v. NPCC's Verification of Mitigation Plan Completion, included as Attachment p-5.

A Form of Notice Suitable for Publication[11]
A copy of a notice suitable for publication is included in Attachment q.

[11] *See* 18 C.F.R. § 39.7(d)(6).

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net Walter Cintron* Manager, Compliance Enforcement Northeast Power Coordinating Council, Inc. 1040 Avenue of the Americas-10th Fl. New York, NY 10018-3703 (212) 840-1070 (212) 302-2782 – facsimile wcintron@npcc.org Edward A. Schwerdt* President & Chief Executive Officer Northeast Power Coordinating Council, Inc. 1040 Avenue of the Americas-10th Fl. New York, NY 10018-3703 (212) 840-1070 (212) 302-2782 – facsimile eschwerdt@npcc.org Stanley E. Kopman* Assistant Vice President of Compliance Northeast Power Coordinating Council, Inc. 1040 Avenue of the Americas-10th Fl. New York, NY 10018-3703 (212) 840-1070 (212) 302-2782 – facsimile skopman@npcc.org	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça* 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 sonia.mendonca@nerc.net *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.

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
Sonia C. Mendonça
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
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity 1, Unidentified Registered Entity 2 and Unidentified Registered Entity 3, and Parent Company
Northeast Power Coordinating Council, Inc.

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition of Violations for URE 1

NPCC, Inc.
NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

ATTACHMENT A

DISPOSITION OF VIOLATION[1]

NERC Tracking Nos.	Regional Entity Tracking No.	NOC#
NPCC200900088, NPCC200900089, NPCC200900090, NPCC200900091, NPCC200900092, NPCC200900096, NPCC200900115 NPCC201000147, NPCC201000148, NPCC201000149, NPCC201000150, NPCC201000151, NPCC201000152	Same	859
Registered Entity: **Unidentified Registered Entity 1**		NERC Registry Id. **NCRXXXXX**
Regional Entity: **Northeast Power Coordinating Council, Inc.**		

VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT (S)	SUB-REQUIREMENT (S)	VRF(S)	VSL(S)
CIP-004-1	2	2.1	Medium	N/A
CIP-004-1	3		Medium	N/A
CIP-004-1	4	4.1	Lower[2]	N/A
CIP-004-1	4	4.2	Medium	N/A
CIP-006-1	2	2.1,2.3	Medium	N/A

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

Violation ID# NPCC201000147 – CIP-004-1 Requirement 2, Sub-Requirement 2.1

The purpose of CIP-004-1 is to ensure the requirement 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.

Text of Reliability Standard and Requirement(s)/Sub-Requirement(s)

R2. Training — The Responsible Entity[3] 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.

(Footnote added).

Possible/Alleged/Confirmed Violation Description

URE-1 self-reported that during a review of required Critical Infrastructure Protection (CIP) Training, they determined that 5 employees with read-only access to the Energy Management System (EMS) did not have the required training prior to the mandatory, July 1, 2009, CIP compliance date for the URE-1.

[3] Within the text of Standard CIP-002 - CIP-009, "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.

A further review was initiated and it was determined that, of the five employees that were non-compliant, 2 of the employees no longer required read only access and their read only access was revoked on January 28, 2010 and February 22, 2010. For the remaining 3 employees that required read-only access, 1 employee completed the required CIP training on January 28, 2010 and the remaining 2 employees completed the required CIP training on February 18, 2010. As a result, NPCC staff finds URE-1 non-compliant with CIP-004-1 Requirement 2, Sub-requirement 2.1.

Reliability Impact Statement - Potential and Actual

NPCC Enforcement determined that the alleged violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the employees did not have unescorted access to the EMS Control Rooms. They were only able to view EMS information remotely and did not have operational control of BPS equipment.

Violation ID# NPCC201000148 – CIP-004-1 Requirement 3

The purpose of CIP-004-1 is to ensure the requirement 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.

Text of Reliability Standard and Requirement(s)/Sub-Requirement(s)

> **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.
>
> > **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.

Possible/Alleged/Confirmed Violation Description
URE-1 self-reported that during a review of required CIP Training, it determined that one of its employees with read only access to the Energy Management System (EMS) did not have the required personnel risk assessment performed within the required time.

A further review determined that this employee no longer required read-only access to the EMS and read only access was revoked on September 30, 2009. URE-1 also performed a personnel risk assessment of the employee and no adverse findings were found.
As a result, NPCC staff finds URE-1 non-compliant with CIP-004-1 Requirement 3.

Reliability Impact Statement - Potential and Actual
NPCC Enforcement determined that the alleged violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS because the employee did not have unescorted access to the EMS Control Rooms. The employee was only able to view EMS information remotely and did not have operational control of BPS equipment.

Violation ID# NPCC201000149 – CIP-004-1 Requirement 4, Sub-Requirement 4.1

The purpose of CIP-004-1 is to ensure the requirement 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.

Text of Reliability Standard and Requirement(s)/Sub-Requirement(s)

> **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.

Possible/Alleged/Confirmed Violation Description
During a quarterly self-assessment of the quarterly access review process, it was determined that the access list generated from the card-key system only allows for one access approver to be linked to an employee's physical access rights, but some employees had been granted access rights by more than one approver. This resulted in incomplete lists of personnel with authorized

unescorted physical access to critical cyber assets along with their specific physical access rights. While the quarterly review did highlight an incomplete list, the self-assessment did not highlight any instances of physical access that were not properly authorized and documented by the access approvers. As a result of the list being incomplete or inaccurate, NPCC staff finds URE-1 non-compliant with CIP-004-1 Requirement 4, Sub-requirement 4.1.

Reliability Impact Statement - Potential and Actual
NPCC Enforcement determined that the alleged violation posed a minimal risk did not create a serious or substantial risk to the bulk power system (BPS). Although the lists generated from the card reader were incomplete, after review by URE-1, it was verified that there were no occurrences of physical access that were not properly authorized and documented by the access approvers.

Violation ID# NPCC200900088, NPCC200900089, NPCC200900090, NPCC2009000 91, NPCC200900115, NPCC201000150, NPCC201000151 - CIP-004-1 Requirement 4, Sub-Requirement 4.2

The purpose of CIP-004-1 is to ensure the requirement 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.

Text of Reliability Standard and Requirement(s)/Sub-Requirement(s)

> **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.

Possible/Alleged/Confirmed Violation Description
On seven occasions, during 2009, URE-1 encountered company personnel not disabling (revoking) employee card keys after that employee no longer required unescorted physical access to critical cyber assets. These events involved 5 employees that were transferred to new positions, 1 employee that retired from the company, and 1 employee that was terminated for cause. The events and duration are as follows:

1. Violation NPCC200900088 - June 14, 2009 – a Substation employee was transferred to a new position and physical access to critical cyber assets was not disabled (revoked) until July 20, 2009. Date of violation – 7/1/2009. Duration of violation – 19 days.
2. Violation NPCC200900089 - June 24, 2009 – a Control Center employee was transferred to a new position and physical access to critical cyber assets was not disabled (revoked) until July 21, 2009. Date of violation – July 1, 2009. Duration of violation – 20 days.
3. Violation NPCC200900090 - July 8, 2009 – a Control Center employee was terminated for cause. Physical access to critical cyber assets was revoked on July 21, 2009. Date of violation July 9, 2009. Duration of violation – 12 days.
4. Violation NPCC200900091 – July 13, 2009 – a Control Center employee was transferred to a new position and physical access to critical cyber assets was not disabled (revoked) until July 21, 2009. Date of violation – July 20, 2009. Duration of violation – 1 day.
5. Violation NPCC200900115 – October 4, 2009 – a Substation employee was transferred to a new position and physical access to critical cyber assets was not disabled (revoked) until October 21, 2009. Date of violation – October 11, 2009. Duration of violation – 10 days.
6. Violation NPCC201000150 – October 1, 2009 – a Substation employee retired and physical access to critical cyber assets was not disabled (revoked) until October 13, 2009. Date of violation – October 8, 2009. Duration of violation – 5 days.
7. Violation NPCC 201000151 – May 1, 2009 – a Substation employee was transferred to a new position and physical access to critical cyber assets was not disabled (revoked) until September 8, 2009. Date of violation – July 1, 2009. Duration of violation 69 days.

Further review showed that the card reader associated with the employee that was terminated for cause was in the possession of a company labor relations manager at the time of termination. Also, the card reader for the employee that retired was in the possession of the employee's supervisor on September 30, 2009, prior to the retirement date of October 1, 2009.

Each one of the revocation requirements was in excess of the timeframe requirements of NERC Standard, CIP-004-1, Requirement 4 Sub-requirement 4.2, therefore, NPCC Enforcement Staff finds URE-1 non-compliant.

Reliability Impact Statement - Potential and Actual

NPCC Enforcement determined that the alleged violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. The reason for this rationale is as follows:

1. For the five employees that no longer required physical access to critical cyber assets, due to transfers, these employees had previously completed the required training and had the required risk assessments performed. Therefore, although not having their card keys disabled, they did not pose a threat to the security of the critical cyber assets or the reliability of the BPS. In all cases related to job transfers, employees did not access critical cyber assets after the effective date of transfer. The duration of violation for four

of the employees was twenty days or less, and for one employee the duration of the violation was 69 days.

2. For the employee that was terminated for cause, the employee's card key was taken from his possession and although the card key was not disabled, the terminated employee no longer had the card key in his possession to allow him physical access to critical cyber assets. Access records indicate that employee did not access critical cyber assets post effective date of termination
3. For the employee that retired, the employee's card key was taken from him prior to his retirement date and separation from the company. Therefore the retried employee no longer had the card key to allow him physical access to critical cyber assets. Access records indicate that employee did not access critical cyber assets post effective date of retirement.

Violation ID# NPCC200900092, 96, NPCC201000152 – CIP-006-1 Requirement 2 Sub Requirement 2.1, 2.3[4]

The Purpose of CIP-006-1 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

Text of Reliability Standard and Requirement(s)/Sub-Requirement(s)

R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

Possible/Alleged/Confirmed Violation Description

During the period from July 27, 2009 through February 20, 2010, URE-1 had three events involving personnel and/or contractors, without authorized physical access to critical cyber

[4] The supporting documents for the CIP-006 R2 (NPCC200900092) violation also references violations of CIP-006 R3.2 (NPCC200900094) and CIP-006 R4.3 (NPCC200900095); NPCC dismissed these violations on March 22, 2010.

assets, accessing these facilities by being provided an access route that was not in conformance with the security perimeter that was installed.

On July 27, 2009, a substation employee with authorized unescorted access to critical cyber assets, card keyed into a physical security perimeter, as per procedure, and then proceeded to prop open the door to allow a pest control contractor to gain access. During this time the pest control contractor, who did not have unauthorized access to Critical Cyber Assets, was not escorted by the company person that provided him access. Propping the door open also created a vulnerability to this location because the perimeter was no longer secure. As part of the physical security perimeter, the substation control house, which stores Critical Cyber Assets, was breached. When the contractor completed his tasks at this location, he removed the cone that had kept the access door propped open, and secured the Critical Cyber Asset perimeter. The employee that provided access was escorting this contractor to multiple substation locations during this day and this was the only infraction that occurred.

On August 12, 2009, a communications company employee used a key, instead of the required card key, to physically access a communications room which is a Critical Cyber Asset. This caused a "key alarm" that was monitored by Security Personnel. This employee was not authorized for unescorted access to Critical Cyber Assets. At the time of the event, key card reader units had been installed and key cards were issued to personnel with authorized unescorted access to allow them to access these facilities. Another mechanism that allowed access to the communication room prior to the effective date of the reliability standard was by use of a key lock, but this was not the method that was supposed to be used. Unfortunately, these locks were not disabled in a way that prevented access to unauthorized personnel who previously had been issued keys.

From February 20, 2010 through February 22, 2010, three security guards, who were not authorized for unescorted physical access to Critical Cyber Assets, used a previously-issued master key, instead of the required card reader, to access a Back-up Control Room. The same three security guards provided escorted access to an asbestos contractor who was involved in building renovations at this facility. Records show that this event occurred nine times during the three day period.

URE-1 has since installed special devices that disable the key locks except to allow access to the communication and back-up control rooms by only authorized individuals at a time when the key card reader unit is inoperable. The keys to these new lock devices were issued only to authorized personnel and are to be used only during emergencies when the key card reader is inoperable. An alarm was also installed to alert security when the special lock key is used to access the communication room.

NPCC Enforcement Staff finds URE-1 non-compliant with CIP-006-1, Requirement 2 Sub-Requirement 2.1, 2.3.

Reliability Impact Statement - Potential and Actual

NPCC Enforcement determined that the alleged violations posed a minimal risk and did not create a serious or substantial risk to the reliability of the BPS. The rationale for this determination is as follows:

1. The contracted personnel that accessed the critical cyber access location were contractors approved by the URE-1 to perform this work.
    a. For the violation involving the pest control contractor, the pest control contractor performs this task on a regular basis, and although having unescorted access to the critical cyber asset facility, he did not have access to the critical cyber equipment. Also, the substation employee that permitted access was in the same control room, but did not have direct eye contact with the pest control contractor.
    b. For the communications employee, as soon as the communications employee accessed the communications room, an alarm was initiated and acknowledged by security. URE-1 personnel, working at the facility were contacted to investigate. It was determined that the communications employee could continue working in the communications room, but needed to be escorted. An authorized company employee remained with the communications employee until he was completed with his task and left the communications room.
    c. In the case of the asbestos contractor, although the security guards that provided escorted access to these contractors were not authorized for unescorted physical access to critical cyber assets, they previously had personal risk assessments performed and 2 of the security guards had the required CIP training.

DISCOVERY INFORMATION

Method of Discovery

Self-Report	☒
Self-Certification	☐
Compliance Audit	☐
Compliance Violation Investigation	☐
Spot Check	☐
Complaints	☐
Periodic Data Submittals	☐
Exception Reporting	☐

Duration Date(s)

Reliability Standard	Violation ID	Violation Start Date	Violation End Date
CIP-004-1	NPCC200900088	7/1/2009	7/20/2009
CIP-004-1	NPCC200900089	7/1/2009	7/21/2009
CIP-004-1	NPCC200900090	7/9/2009	7/21/2009
CIP-004-1	NPCC200900091	7/20/2009	7/21/2009
CIP-004-1	NPCC200900115	10/11/2009	10/21/2009
CIP-004-1	NPCC201000147	7/1/2009	2/18/2010

CIP-004-1	NPCC201000148	7/1/2009	9/30/2009
CIP-004-1	NPCC201000149	10/1/2009	5/15/2010
CIP-004-1	NPCC201000150	10/8/2009	10/13/2009
CIP-004-1	NPCC201000151	7/1/2009	9/8/2009
CIP-006-1	NPCC200900092	7/27/2009	7/27/2009
CIP-006-1	NPCC200900096	8/12/2009	8/12/2009
CIP-006-1	NPCC201000152	2/20/2010	2/22/2010

Date Discovered by or Reported to Regional Entity

Violation ID	Date Discovered by or Reported to Regional Entity
NPCC200900088,89,90,91	Self-Report
NPCC200900092	Self-Report
NPCC200900096	Self-Report
NPCC200900115	Self-Report
NPCC201000147,148,149,150,151,152	Self-Report

Is the issue still occurring? Yes ☐ No ☒
Remedial Action Directive Yes ☐ No ☒
Pre to Post June 21, 2007 violation Yes ☐ No ☒

MITIGATION INFORMATION

	CIP-004-1	CIP-006-1	CIP-006-1	CIP-004-1
Violation Tracking Number	NPCC200900088,89, 90,91	NPCC2000900092	NPCC200900096	NPCC2009000115
Mitigation Plan ID	MIT-09-2356	MIT-09-2357	MIT-09-2358	MIT-09-2399
Date Submitted to Regional Entity	2/19/2010	2/19/2010	2/21/2010	3/10/2010
Date Accepted by Regional Entity	3/5/2010	3/5/2010	3/5/2010	3/16/2010
Date Approved by NERC	3/10/2010	3/10/2010	3/10/2010	3/24/2010
Date Provided to FERC	3/5/2010	3/5/2010	3/5/2010	3/19/2010
Complete?	Yes	Yes	Yes	Yes

Expected Completion Date	8/31/2009	8/31/2009	11/13/2009	1/31/2010
Extensions granted	No	No	No	No
Actual Completion Date	8/31/2009	8/31/2009	11/13/2009	1/31/2010
Date of Certification Letter	10/22/2010	10/22/2010	10/26/2010	12/2/2010
Date of Verification Letter	1/26/2011	1/26/2011	1/26/2011	1/26/2011

	CIP-004-1	CIP-004-1	CIP-004-1	CIP-004-1
Violation Tracking Number	NPCC201000147,148	NPCC201000149	NPCC201000150	NPCC201000151
Mitigation Plan ID	MIT-09-2578	MIT-09-2579	MIT-09-2580	MIT-09-2581
Date Submitted to Regional Entity	5/20/2010	5/20/2010	5/20/2010	5/20/2010
Date Accepted by Regional Entity	5/26/2010	5/26/2010	5/26/2010	5/26/2010
Date Approved by NERC	6/27/2010	6/27/2010	6/27/2010	6/27/2010
Date Provided to FERC	5/28/2010	5/28/2010	5/28/2010	5/28/2010
Complete?	Yes	Yes	Yes	Yes
Expected Completion Date	2/22/2010	5/30/2010	5/15/2010	5/15/2010
Extensions granted	No	No	No	No
Actual Completion Date	2/22/2010[5]	5/30/2010	5/15/2010	5/15/2010

[5] The Certification of Completion incorrectly states that the CIP-004 violations were mitigated on May 20, 2010.

Date of Certification Letter	11/12/2010	12/2/2010	10/27/2010	10/26/2010
Date of Verification Letter	1/26/2011	1/26/2011	1/26/2011	1/26/2011

	CIP-006-1			
Violation Tracking Nimber	NPCC201000152			
Mitigation Plan ID	MIT-10-2582			
Date Submitted to Regional Entity	5/20/2010			
Date Accepted by Regional Entity	5/26/2010			
Date Approved by NERC	6/27/2010			
Date Provided to FERC	5/28/2010			
Complete?	Yes			
Expected Completion Date	5/7/2010			
Extensions granted	No			
Actual Completion Date	5/7/2010			
Date of Certification Letter	10/22/2010			
Date of Verification Letter	1/26/2011			

CIP-004-1 - Requirement 4, Sub-Requirement 4.2 NPCC200900088, 89, 90, 91

Action taken to Mitigate the Issue
URE-1's Mitigation Plan was to enhance the awareness of the requirements of Cyber Security requirements. Actions taken were:

1. Employees directly responsible for access revocations had the incidents discussed with them.
2. A high importance e-mail was distributed to all authorized access approvers and responsible managers regarding access and revocation of access.
3. Security sent a cyber security – physical security incident notice to all authorized access approvers and responsible managers to increase awareness and "lessons learned" training opportunities.
4. Additional CIP awareness training was conducted.

List of Evidence reviewed by Regional Entity
URE-1 provided the following evidence:

1. E-mail documents, dated 7/28/09 and 7/29/09, that were distributed to managers and access approvers discussing the incidents involved and the requirements for the revocation of authorized access to critical cyber assets.
2. Documentation provided that Managers discussed requirements and responsibilities for the NERC CIP standards at monthly staff meetings.

CIP-006-1- Requirement 2, Sub-Requirement 2.3 NPCC2000900092

Actions taken to Mitigate the Issue
URE-1's Mitigation Plan was to enhance the awareness of Cyber Security requirements. Actions taken were:

1. Incident was discussed with employee involved in the incident.
2. Security sent a cyber security – physical security incident notice to all authorized access approvers and responsible managers regarding the physical security perimeter door that was propped open.
3. Additional CIP awareness training was conducted.

List of Evidence reviewed by Regional Entity
URE-1 provided the following evidence:

1. A document summarizing the discussion of the incident with the employee involved with the violation.
2. E-mail document that was distributed to managers and access approvers discussing the incident involved and the requirements for physical access to critical cyber assets.

3. Documentation provided that Managers discussed requirements and responsibilities for the NERC CIP standards at the monthly staff meetings.

CIP-004-1 – Requirement 4, Sub-Requirement 4.2 NPCC200900115

Actions taken to Mitigate Issue
URE-1's Mitigation Plan was to enhance the awareness of Cyber Security requirements. In addition, a report was to be developed to provide an additional tool for review of employees that should have access to Critical Cyber Assets. Actions taken were:

1. Employee directly responsible for the access revocation had the incident discussed with him.
2. A high importance e-mail was sent out to all authorized access approvers and responsible managers regarding access and revocation of access.
3. Security sent a cyber security – physical security incident notice to all authorized access approvers and responsible managers to increase awareness and "lessons learned" training opportunities.
4. Implementation of employee transfer reports to provide an additional review regarding employees that should have their access to critical cyber access revoked.

List of Evidence reviewed by Regional Entity
URE-1 provided the following evidence:

1. E-mail document verification that the incident was discussed with the employee directly responsible for access revocation.
2. E-mail document that was distributed to managers and access approvers discussing the incidents involved and the requirements for the revocation of authorized access to critical cyber assets.
3. E-mail documenting the rollout of the employee transfer report implementation, along with a training document describing the implementation process.

CIP-004-1 – Requirement 2, Sub-Requirement 2.1 and Requirement 3 NPCC201000147, 148

Actions taken to Mitigate Issue
URE-1's Mitigation Plan was to complete a detailed review of personnel with access to the Energy Management System to ensure all training and personnel risk assessments were complete and up to date. Actions taken were:

1. A full review of access to the Energy Management System was performed.
2. The status of CIP Training and Personnel Risk Assessments for all employees with access to the Energy Management System was confirmed.

3. CIP Training was completed where required or access to the Energy Management System was revoked where access was no longer required.

List of Evidence reviewed by Regional Entity
URE-1 provided the following evidence:

1. Document showing a list of approved personnel access to cyber assets and approved access roles.
2. Document showing employee approved access and last date Personal Risk Assessment and CIP training was completed. This document showed the employees that were delinquent with their required training and/or Personal Risk Assessment.
3. Document showing the status of the employees that were delinquent with CIP training and Personal Risk Assessment; dates for revocation of physical access to critical cyber assets for these employees, required training and Personal Risk Assessments completed.

CIP-004-1 – Requirement 4, Sub-Requirement 4.1 NPCC201000149

Actions taken to Mitigate Issue
URE-1's Mitigation Plan was to improve the access list documentation to assure accuracy of the access lists of personnel authorized for physical access to Critical Cyber Assets. Actions taken were:

1. Complete scheduled quarterly review with the reports generated from the current system.
2. A reporting database was created that produces complete lists of personnel with authorized unescorted physical access to Critical Cyber Assets, including individual physical access rights to those Critical Cyber Assets. The reporting database is reconciled to the card key system on a monthly basis.
3. Started quarterly access reviews with the complete lists of personnel with authorized unescorted physical access to Critical Cyber Assets, including their specific access rights to those Critical Cyber Assets.

List of Evidence reviewed by Regional Entity
URE-1 provided the following evidence:

1. Documentation showing a completed quarterly review form.
2. A process document for the reporting database along with a sampling of the reporting database documentation.
3. A sampling of a completed quarterly physical access to critical cyber assets form along with a sampling of a list of personnel with physical access to critical cyber assets.

CIP-004-1 – Requirement 4, Sub-Requirement 4.2 NPCC201000150, 151

Actions taken to Mitigate Issue

URE-1's Mitigation Plan was improve the process for revocation of personnel no longer requiring physical access to Critical Cyber Assets. Actions taken were:

1. Employee directly responsible for the access revocation had the incident discussed with him.
2. A high importance e-mail was sent out to all authorized access approvers and responsible managers regarding access and revocation of access.
3. Security sent a cyber security – physical security incident notice to all authorized access approvers and responsible managers to increase awareness and "lessons learned" training opportunities.
4. Employee transfer reports were made available to the responsible managers. The employee transfer reports are an additional method to assist in identifying employees that should have their access to Critical Cyber Assets revoked.
5. CIP Awareness Training was conducted during March through May, 2010. These training sessions were in addition to the required annual training program.
6. Security developed a procedure to perform a centralized review of the employee transfer reports.
7. Security will be responsible to revoke unescorted physical access to Critical Cyber Assets when required.

List of Evidence reviewed by Regional Entity

URE-1 provided the following evidence:

1. E-mail document verification that the incident was discussed with the employees directly responsible for access revocation.
2. E-mail document that was distributed to managers and access approvers discussing the incidents involved and the requirements for the revocation of authorized access to critical cyber assets.
3. E-mail documenting the rollout of the employee transfer report implementation, along with a training document describing the implementation process.
4. Documents showing the presentation presented during the period of March to May, 2010 along with the schedule of training sessions.
5. Document showing the procedure for the Security revocation of employee who no longer requires authorized unescorted physical access to critical cyber assets.

CIP-006-1 Requirement 2, Sub-Requirement 2.1 NPCC200900096

Actions taken to Mitigate Issue
URE-1's Mitigation Plan was to heighten CIP awareness and restrict physical authorized access to Critical Cyber Assets to their card reader system only. Actions taken were:

1. Incident was discussed with the communications company employee that was involved in the incident.
2. Security sent a cyber security – physical security incident notice to all authorized access approvers and responsible managers.
3. Additional CIP awareness training was conducted.
4. Locks and keys at communication facilities, which contain Critical Cyber Assets, were replaced with special locks and keys for these locks will be restricted. The special lock system will be during emergencies, when the card reader system becomes inoperable.
5. An alarm was installed, that will be initiated whenever a special lock system is utilized.

List of Evidence reviewed by Regional Entity
URE-1 provided the following evidence:

1. An incident report showing a description of the event, discussion with the communication employee involved with the incident, and recommended follow-up actions to mitigate further occurrences of the violation.
2. E-mail document that was distributed to managers and access approvers discussing the incident involved and the requirements for personnel not authorized for physical access to critical cyber assets to escorted at all times.
3. Documentation provided that Managers discussed requirements and responsibilities for the NERC CIP standards at the monthly staff meetings.
4.

CIP-006-1 Requirement 2 NPCC201000152

Actions taken to Mitigate issue
URE-1's Mitigation Plan was to heighten CIP awareness and restrict physical authorized access to Critical Cyber Assets to its card reader system only at all Critical Cyber Access locations. This would bring the entity into compliance with CIP-006-1, requirement 2. Actions taken were:

1. The incident was discussed with the three security guards involved in the incident.
2. The security guards were required to read and initial a memorandum regarding the incident.

3. Controlled Access Area signs were installed, along with instructions, at the Back-up Control Room door.
4. Lock cores were disabled with the use of block-out blades. Access to the block-out blade key is restricted.
5. The security Guard that was not CIP trained, completed CIP training.
6. Block-out blades were installed at all NERC CIP locations.

List of Evidence reviewed by Regional Entity
URE-1 provided the following evidence:

1. Document showing the review of the incident and requirements concerning cyber access with the affected security guards along with a sign-off verifying review was completed.
2. Document showing a picture of the Controlled Access Area sign added to the Back-up Control Room Door stating CIP requirements for access. Also, attestations that Controlled Access Area signs were installed at all NERC CIP doors.
3. E-mail stating that Lock Cores were disabled with the installation of blockout blades at the Back-up control room and access keys are restricted and security receives an alarm when these keys are used.
4. Document showing a sign-off sheet for security guards completing required CIP training.
5. E-mail documenting that blockout blades were installed at all URE-1 NERC CIP location.

PENALTY INFORMATION

Proposed Penalty or Sanction $80,000.00 for 21 total violations

NPCC has determined that a penalty of $80,000.00 bears a reasonable relationship to the severity of the violation and considers the actions taken by URE-1, URE-2 and URE-3 to mitigate the violations. This determination is based on the following facts:

- URE-1, URE-2 and URE-3 self reported the alleged violations;
- There is no evidence that URE-1, URE-2 and URE-3 made any attempt to conceal the alleged violations;
- URE-1, URE-2 and URE-3 fully cooperated with NPCC, willingly discussed the alleged violation and provided additional information regarding the alleged violations;
- NPCC determined the violations did not pose a serious or significant risk to the BPS as discussed above.

This proposed penalty or sanction is subject to review and possible revision by NERC and FERC. NERC will include its determination of the proposed penalty or sanction in a Notice of Proposed Penalty or Sanction to be filed with FERC.

(1) Registered Entity's compliance history

Prior violations of this Reliability Standard or Requirement(s) thereunder?
Yes ☐ No ☐
Number of such violations?

List any confirmed or settled violations and status

Prior violations of other Reliability Standard(s) or Requirements thereunder?
Yes ☐ No ☐
Number of such violations?

List any prior confirmed or settled violations and status

(2) The degree and quality of cooperation by the Registered Entity

Full cooperation Yes ☒ No ☐
Explain
URE-1 personnel were very responsive in providing information to NPCC upon request.

(3) The presence and quality of the Registered Entity's compliance program

Is there a compliance program Yes ☒ No ☐
Explain
URE-1, URE-2, and URE-3 are subsidiaries of a parent company and have an active comprehensive regulatory compliance program as part of the parent company network.

Is senior management supportive Yes ☒ No ☐
Explain

(4) Any attempt by the Registered Entity to conceal the violation or information needed to review, evaluate or investigate the violation
Yes ☐ No ☒
Explain

(5) Any evidence this was an intentional violation
Yes ☐ No ☒
Explain

(6) Any other extenuating circumstances

Yes ☐ No ☒

Explain

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition of Violations for URE 2

NPCC, Inc.
NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

ATTACHMENT B

DISPOSITION OF VIOLATION[1]

NERC Tracking Nos.	Regional Entity Tracking No.	NOC#
NPCC2009000103, NPCC200900104, NPCC200900105, NPCC200900114, NPCC201000146, NPCC201000156	Same	859
Registered Entity: **Unidentified Registered Entity 2**		NERC Registry Id. **NCRXXXXX**
Regional Entity: **Northeast Power Coordinating Council, Inc.**		

VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	4	4.1	Lower	N/A
CIP-004-1	4	4.2	Medium	N/A
CIP-006-1	2	2.1,2.3	Medium	N/A
CIP-006-2	4		Medium	Moderate

Violation ID# NPCC201000146 – CIP-004-1 Requirement 4 Sub-Requirement 4.1

The purpose of CIP-004-1 is to ensure the requirement 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.

Text of Reliability Standard and Requirement(s)/Sub-Requirement(s)

> **R4.** Access — The Responsible Entity[2] 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.

[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.

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.

(Footnote added).

Possible/Alleged/Confirmed Violation Description

During a quarterly self-assessment of the quarterly access review process, it was determined that the access list generated from the card-key system only allows for one access approver to be linked to an employee's physical access rights, but some employees had been granted access rights by more than one approver. This resulted in incomplete lists of personnel with authorized unescorted physical access to critical cyber assets along with their specific physical access rights. While the quarterly review did highlight an incomplete list, the self-assessment did not highlight any instances of physical access that were not properly authorized and documented by the access approvers. As a result of the list being incomplete or inaccurate, NPCC staff finds URE-2 non-compliant with CIP-004-1 Requirement 4, Sub-requirement 4.1.

Reliability Impact Statement - Potential and Actual

NPCC Enforcement determined that the alleged violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although the lists generated from the card reader were incomplete, review by URE-2 verified that there were no occurrences of physical access that were not properly authorized and documented by the access approvers. URE-2, as part of its Mitigation Plan, has developed a reporting database that will produce complete lists of personnel with authorized unescorted physical access to critical cyber assets, and it will be reconciled to the card reader system on a monthly basis.

Violation ID# NPCC200900103 - CIP-004-1 Requirement 4 Sub-Requirement 4.2

The purpose of CIP-004-1 is to ensure 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.

[2] Within the text of Standard CIP-002 - CIP-009, "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.

Text of Reliability Standard and Requirement(s)/Sub-Requirement(s)

> **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.

Possible/Alleged/Confirmed Violation Description

During 2009, URE-2 discovered an incident involving company personnel not revoking an employee's card key after the employee no longer required unescorted physical access to critical cyber assets. On July 20, 2009, an employee with authorized cyber and authorized unescorted physical access to critical cyber assets transferred to a new position that did not require this access. The employee's access was revoked on August 20, 2009. As required by NERC Reliability Standard CIP-004-1, Requirement 4.2, access rights for this employee should have been revoked within 7 days from when the employee no longer required access to Critical Cyber Assets. The actual revocation of access rights for this employee was 31 days, which was in excess of the timeframe requirements of NERC Standard, CIP-004-1, Requirement 4 Sub-requirement 4.2. Therefore NPCC Enforcement Staff finds URE-2 non-compliant.

Reliability Impact Statement - Potential and Actual

NPCC Enforcement determined that the alleged violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS because follow-up investigations performed by the URE-2 confirmed that the employee that no longer required physical access rights to Critical Cyber Assets did not access any area containing Critical Cyber Assets after July 20, 2009.

Violation ID# NPCC200900104, 105, 114 – CIP-006-1 Requirement 2, Sub-Requirements 2.1, 2.2

The Purpose of CIP-006-1 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

Text of Reliability Standard and Requirement(s)/Sub-Requirement(s)

> **R2.** Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week.
>
> > **R2.1.** Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
> >
> > **R2.2.** Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
> >
> > **R2.3.** Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
> >
> > **R2.4.** Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

Possible/Alleged/Confirmed Violation Description

During the period from August 19, 2009 through December 2, 2009, URE-2 had three events involving company personnel without authorized physical access to critical cyber assets accessing these facilities by being provided an access route that was not in conformance with the security perimeter that was installed.

Prior to the effective date of the reliability standards, locks and keys had been used in areas that later became part of the security perimeter. On August 19, 2009 there were 2 events involving substation employees not authorized for unescorted access to Critical Cyber Assets. The first event involved an employee using a key that previously had been provided, instead of the required card key, to access a substation control house physical security perimeter. The second event also involved two employees using a key that previously had been provided, instead of the required card key, to access a substation control house physical security perimeter. In both instances, a "key alarm" was generated to Security Personnel.

The December 2, 2009 incident involved a contractor using a key that had previously been provided, instead of the required card key, to access a substation control house physical security perimeter. A key alarm was also generated to Security Personnel for this event.

URE-2 has since installed special devices that disable the key locks except to allow access to critical substations by authorized individuals only at a time when the key card reader unit is inoperable. The keys to these new lock devices were issued only to authorized personnel and are to be used only during emergencies when the key card reader is inoperable.

As a result of company personnel accessing Critical Cyber Assets by use of access keys not designed for operational control of these Critical Cyber Assets, NPCC staff finds URE-2 non-compliant with CIP-006-1 Requirement 2, Sub-Requirement 2.1, 2.2.

Reliability Impact Statement - Potential and Actual
NPCC Enforcement determined that the alleged violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. The rationale for this determination is that in all instances, an alarm was initiated and addressed by security.

Violation ID# NPCC201000156 – CIP-006-2 Requirement 4

The Purpose of CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

Text of Reliability Standard and Requirement(s)/Sub-Requirement(s)

> **R4.** Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
> - Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
> - Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
> - Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
> - Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

Possible/Alleged/Confirmed Violation Description
On May 8 and 9, 2010, two unauthorized access incidents occurred at the URE-2's vacant former Control Room.

Prior to the effective date of the reliability standards, locks and keys had been used in areas that later became part of the security perimeter.

On May 8, 2010, a facilities employee, who was not authorized for unescorted physical access to Critical Cyber Assets, used a master key that previously had been provided to bypass the card key access system to access the vacant former Control Room. The facility employee was responding to a cooling water high temperature alarm for the Energy Management System computer room.

On May 9, 2010, a facilities employee, who was not authorized for unescorted physical access to Critical Cyber Assets, used a master key that previously had been provided to bypass the card key access system to access the vacant former Control Room. The facility employee was responding to a cooling water high temperature alarm for the Energy Management System computer room.

The former Control Room operation had moved to a new facility. At the time of the events, the former Control Room still contained one Energy Management System workstation that is a Critical Cyber Asset, and the facility was still considered to be a Critical Asset.

URE-2 has since installed special devices that disable the key locks except to allow access to the former control room by authorized individuals only at a time when the key card reader unit is inoperable. The keys to these new lock devices were issued only to authorized personnel and are to be used only during emergencies when the key card reader is inoperable.

As a result of company personnel accessing Critical Cyber Assets by use of access keys not designed for operational control of these Critical Cyber Assets, NPCC staff finds URE-2 non-compliant with CIP-006-1 Requirement 2.

Reliability Impact Statement - Potential and Actual

NPCC Enforcement determined that the alleged violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. The rationale for this determination is that in all instances, an alarm was initiated and addressed by security and the facility employee did not have electronic access to the critical cyber assets.

DISCOVERY INFORMATION

Method of Discovery

Self-Report	☒
Self-Certification	☐
Compliance Audit	☐
Compliance Violation Investigation	☐
Spot Check	☐
Complaints	☐
Periodic Data Submittals	☐
Exception Reporting	☐

Duration Date(s)

Reliability Standard	Violation ID	Violation Start Date	Violation End Date
CIP-004-1	NPCC201000146	10/1/2009	5/30/2010
CIP-004-1	NPCC200900103	7/27/2009	8/20/2009
CIP-006-1	NPCC200900104	8/19/2009	11/9/2009
CIP-006-1	NPCC200900105	8/19/2009	11/9/2009

CIP-006-1	NPCC200900114	12/2/2009	12/4/2009
CIP-006-2	NPCC201000156	5/8/2010	5/28/2010

Date Discovered by or Reported to Regional Entity

Violation ID	Date Discovered by or Reported to Regional Entity
NPCC200900103,104,105	Self-Report
NPCC200900114	Self-Report
NPCC201000146	Self-Report
NPCC201000156	Self-Report

Is the issue still occurring? Yes ☐ No ☒
Remedial Action Directive Yes ☐ No ☒
Pre to Post June 18, 2007 violation Yes ☐ No ☒

MITIGATION INFORMATION

	CIP-004-1	CIP-004-1	CIP-006-1	CIP-006-1
Violation Tracking Number	NPCC201000146	NPCC200900103	NPCC200900104,5	NPCC200900114
Mitigation Plan ID	MIT-09-2577	MIT-09-2359	MIT-09-2360	MIT-092398
Date Submitted to Regional Entity	5/20/2010	2/21/2010	2/21/2010	3/10/2010
Date Accepted by Regional Entity	5/26/2010	3/5/2010	3/5/2010	3/16/2010
Date Approved by NERC	6/27/2010	3/10/2010	3/10/2010	3/24/2010
Date Provided to FERC	7/1/2010	3/10/2010	3/10/2010	3/24/2010
Complete?	Yes	Yes	Yes	Yes
Expected Completion Date	5/30/2010	8/31/2009	11/9/2009	12/4/2009
Extensions granted	No	No	No	No
Actual Completion Date	5/30/2010	8/31/2009	11/9/2009	12/4/2009

Date of Certification Letter	12/2/2010	12/3/2010	12/2/2010	12/3/2010
Date of Verification Letter	1/26/2011	1/26/2011	1/26/2011	1/26/2011

	CIP-006-2			
Violation Tracking System	NPCC201000156			
Mitigation Plan ID	MIT-10-2933			
Date Submitted to Regional Entity	9/30/2010			
Date Accepted by Regional Entity	10/1/2010			
Date Approved by NERC	10/27/2010			
Date Provided to FERC	10/27/2010			
Complete?	Yes			
Expected Completion Date	6/28/2010			
Extensions granted	No			
Actual Completion Date	6/28/2010			
Date of Certification Letter	12/3/2010			
Date of Verification Letter	1/26/2011			

CIP-004-1 – Requirement 4, Sub-Requirement 4.1 NPCC201000146

Actions Taken to Mitigate the Issue
URE-2's Mitigation Plan required it to:

1. Perform scheduled quarterly reviews to ensure existing physical access is appropriate.
2. Create a reporting database that will produce complete lists of personnel with authorized unescorted access to Critical Cyber Assets, including their specific physical access rights to Critical Cyber Assets. The reporting database will be reconciled to the card key system on a monthly basis.
3. Commence quarterly access reviews with complete lists of personnel with authorized unescorted access to Critical Cyber Assets, including their specific access rights to Critical Cyber Assets.

List of Evidence reviewed by Regional Entity
URE-2 provided the following evidence:

1. Documentation showing a completed quarterly review form.
2. A process document for the reporting database along with a sampling of the reporting database documentation.
3. A sampling of a completed quarterly physical access to critical cyber assets form along with a sampling of a list of personnel with physical access to critical cyber assets.

CIP-004-1 – Requirement 4, Sub-Requirement 4.2 NPCC200900103

Actions Taken to Mitigate the Issue
URE-2's Mitigation Plan required it to:

1. Discuss incident with employees directly responsible for the access revocation.
2. Distribute a high importance e-mail to all authorized access approvers and responsible managers regarding access and revocation of access.
3. Security sent a cyber security – physical security incident notice to all authorized access approvers and responsible managers to increase awareness and "lessons learned" training opportunities.
4. Perform additional CIP awareness training per request of senior management.

List of Evidence reviewed by Regional Entity
URE-2 provided the following evidence:

1. E-mail document verification that the incident was discussed with the employee directly responsible for access revocation.

2. E-mail document that was distributed to managers and access approvers discussing the incidents involved and the requirements for the revocation of authorized access to critical cyber assets.
3. Documentation provided that Managers discussed requirements and responsibilities for the NERC CIP standards at the monthly staff meetings.

CIP-006-1 – Requirement 2, Sub-Requirement 2.2 – NPCC200900104, 105

Actions Taken to Mitigate the Issue
URE-2's Mitigation Plan required it to:

1. Discuss incident with the employees that were involved.
2. Have Security send a cyber security – physical security incident notice to all authorized access approvers and responsible managers.
3. Perform additional CIP awareness training per request of senior management.
4. Produce an educational security video including information regarding critical infrastructure protection.
5. Create Critical Infrastructure Protection talking points for discussion with employees during safety briefings.
6. Develop a video for use including a section regarding CIP Standards and the importance with the CIP standards. Senior executives are to deliver this message.
7. Special lock cores to be disabled with blockout blades. Access to the blockout extractor keys for these special locks will be restricted. Access via these special locks will only be permitted during emergency situations.

List of Evidence reviewed by Regional Entity
URE-2 provided the following evidence:

1. E-mail document verification that the incident was discussed with the employees involved.
2. E-mail document that was distributed to managers and access approvers discussing the incidents involved and the requirements for physical access to critical cyber assets.
3. At a monthly staff meeting, Managers discuss requirements and responsibilities for the NERC CIP standards.The video provided that incorporates requirements of CIP standards.
4. A document that explains the physical access requirements of the CIP-006 standard.
5. E-mail documenting that blockout blades were installed at the URE-2 Company NERC CIP location.

CIP-006-1 – Requirement 2, Sub-Requirement 2.1 – NPCC200900114

Actions Taken to Mitigate the Issue
URE-2's Mitigation Plan required it to:

1. The incident was discussed with the contractor's company.
2. Special lock cores were disabled with the use of blockout blades. Access to the blockout blade extractor keys for these special locks is restricted. Special lock key access is permitted only in an emergency if the card key system is inoperable. The use of a special lock key causes an alarm that is monitored by security.

List of Evidence reviewed by Regional Entity
URE-2 provided the following evidence:

1. An incident report showing report of incident, and discussion of personnel involved.
2. E-mail document certifying the blockout blades were installed at the station.

CIP-006-2 – Requirement 4 – NPCC201000156

Actions Taken to Mitigate the Issue
URE-2's Mitigation Plan required it to:

1. Discuss the incidents with the two Facilities employees involved with the unauthorized access incidents.
2. Lock cores to be changed at the former Control Room. Key access will only be gained by the use keys which are controlled by employees who are authorized for unescorted access to critical cyber assets.
3. Install lock-out blades that fit the new lock cores at the former Control Room.
4. Perform a training session with Facilities employees to enhance awareness of critical infrastructure protection compliance requirements.

List of Evidence reviewed by Regional Entity
URE-2 provided the following evidence:

1. E-mail document attesting that the incident was discussed with the 2 facilities employees involved with the unauthorized access incidents and lock cores were changed.
2. E-mail document verification that lock-out blades were installed at the former Control Room.
3. E-mail document attesting that CIP awareness training was administered to facilities management employees.

PENALTY INFORMATION

Proposed Penalty or Sanction (SEE Attachment A, URE-1 Disposition)

(1) Registered Entity's compliance history

Prior violations of this Reliability Standard or Requirement(s) there under?

Yes ☐ No ☐

Number of such violations?

List any confirmed or settled violations and status

Prior violations of other Reliability Standard(s) or Requirements there under?

Yes ☐ No ☐

Number of such violations?

List any prior confirmed or settled violations and status

(2) The degree and quality of cooperation by the Registered Entity

Full cooperation Yes ☒ No ☐

Explain

(3) The presence and quality of the Registered Entity's compliance program

Is there a compliance program Yes ☒ No ☐

Explain

See Attachment A, URE-1 Disposition Document for Compliance Program.

Is senior management supportive Yes ☒ No ☐

Explain

See Attachment A, URE-1 Disposition Document for Compliance Program.

(4) Any attempt by the Registered Entity to conceal the violation or information needed to review, evaluate or investigate the violation

Yes ☐ No ☒

Explain

(5) Any evidence this was an intentional violation

Yes ☐ No ☒

Explain

(6) Any other extenuating circumstances

Yes ☐ No ☒

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition of Violations for URE 3

NPCC, Inc.
NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

ATTACHMENT C

DISPOSITION OF VIOLATION[1]

NERC Tracking Nos.	Regional Entity Tracking No.	NOC#
NPCC201000181 **NPCC201000182**	Same	859
Registered Entity: **Unidentified Registered Entity 3**		NERC Registry Id. **NCRXXXXX**
Regional Entity: **Northeast Power Coordinating Council, Inc.**		

VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)	
CIP-004-2	4	4.2	Medium	Moderate	

Violation ID# NPCC201000181, 182 – CIP-004-2 Requirement 4, Sub-requirement R4.2

The purpose of CIP-004-2 is to ensure the requirement 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.

Text of Reliability Standard and Requirement(s)/Sub-Requirement(s)

> **R4.** Access — The Responsible Entity[2] 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

[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.
[2] Within the text of Standard CIP-002 - CIP-009, "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.

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.

(Footnote added).

Possible/Alleged/Confirmed Violation Description

On two occasions, during June of 2010, URE-3 discovered that company personnel had not revoked employee/contractor card keys after that employee/contractor no longer required unescorted physical access to Critical Cyber Assets. These events involved 1 employee that retired and 1 contractor that left the company under contract. The events and duration are as follows:

On June 1, 2010, a contractor employee, performing services for URE-3 and having authorized unescorted physical access to URE-3 critical cyber assets, left his company in which he was employed. The employee's access was revoked on June 14, 2010. Date of violation – 6/8/2010. Duration of violation – 6 days.

On June 30, 2010 an employee with authorized unescorted physical access to critical cyber assets retired from the company. The employee's access was revoked on August 5, 2010. Date of violation - July 7, 2010. Duration of violation – 29 days.

As required by NERC Reliability Standard CIP-004-2, Requirement 4, Sub-requirement 4.2, access rights for these employees should have been revoked within 7 days from when the employee/contractor no longer required access to Critical Cyber Assets. The actual revocations of access rights for these employees were, respectively, 6 days and 29 days in excess of the 7 day timeframe requirements of NERC Standard, CIP-004-2, Requirement 4 Sub-requirement 4.2. Therefore NPCC Enforcement Staff finds URE-3 non-compliant.

Reliability Impact Statement - Potential and Actual

NPCC Enforcement determined that the alleged violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because follow-up investigations performed by URE-3 confirmed that the employee and contractor that no longer required physical access rights to Critical Cyber Assets did not access any area containing Critical Cyber Assets after June 1, 2010 (contractor) and June 30, 2010 (employee).

DISCOVERY INFORMATION

Method of Discovery

Self-Report	☒
Self-Certification	☐
Compliance Audit	☐
Compliance Violation Investigation	☐
Spot Check	☐
Complaints	☐
Periodic Data Submittals	☐
Exception Reporting	☐

Duration Date(s)

Reliability Standard	Violation ID	Violation Start Date	Violation End Date
CIP-004-2	NPCC201000181	6/8/2010	6/14/2010
CIP-004-2	NPCC201000182	7/7/2010	8/5/2010

Date Discovered by or Reported to Regional Entity Self-Report

Is the issue still occurring?	Yes	☐	No	☒
Remedial Action Directive	Yes	☐	No	☒
Pre to Post June 18, 2007 violation	Yes	☐	No	☒

MITIGATION INFORMATION

	CIP-004-2
Violation Tracking Number	NPCC201000181,82
Mitigation Plan ID	MIT-10-3404
Date Submitted to Regional Entity	12/22/2010
Date Accepted by Regional Entity	1/12/2011
Date Approved by NERC	3/15/2011
Date Provided to FERC	3/15/2011
Complete?	Yes
Expected Completion Date	12/21/2010
Extensions granted	No
Actual Completion Date	12/20/2010
Date of Certification Letter	3/14/2011
Date of Verification Letter	4/5/2011

CIP-004-2 – Requirement 4, Sub-Requirement 4.2 NPCC201000181, 183

Actions Taken to Mitigate the Issue

URE-3's Mitigation Plan required it to:

1. Employees directly responsible for the access revocation had the incident discussed with them. The need for compliance was reinforced.
2. The responsible URE-3 Manager communicated with the contractor's management re-emphasizing the contractual need to remain CIP compliant generally and notify parent company immediately of any changes in status of employees with physical access to Critical Cyber Assets specifically.
3. A high importance e-mail was sent to all authorized access approvers and responsible managers regarding access and revocation of access.
4. Additional critical infrastructure protection awareness training was conducted.
5. Add responsible Generation authorization approvers to the daily distribution lists of contractor and employee employment status change reports.
6. The Security department will be responsible for the centralized review of employee transfer reports. Security will revoke unescorted physical access to critical cyber assets when required. The Security department will write a procedure for this process.

List of Evidence reviewed by Regional Entity

URE-3 provided the following evidence:

1. E-mail document confirming that, 3 employees responsible for revocation had the incidents discussed with them and procedural requirements with CIP-004 for revocation were re-enforced.
2. E-mail document that was sent to responsible unescorted physical access approvers re-enforcing the requirements for revocation and the importance of doing so in a timely manner as required by the CIP-004 standard .
3. E-mail document confirming that the contracted employees had the requirements of CIP-004 R4.2 discussed with them.
4. A training document showing training for CIP standards and a list of attendees.
5. E-mail document requesting additional personnel to be added to the access approver list and a sampling of the computerized notification list showing personnel added.
6. Procedure for Security instructing on their responsibilities for revoking access.

PENALTY INFORMATION

Proposed Penalty or Sanction **(See Attachment A, URE-1 Disposition Doc.)**

(1) Registered Entity's compliance history

Prior violations of this Reliability Standard or Requirement(s) there under?

Yes ☐ No ☐

Number of such violations?

List any confirmed or settled violations and status

Prior violations of other Reliability Standard(s) or Requirements there under?

Yes ☐ No ☐

Number of such violations?

List any prior confirmed or settled violations and status

(2) The degree and quality of cooperation by the Registered Entity

Full cooperation Yes ☒ No ☐

Explain

(3) The presence and quality of the Registered Entity's compliance program

Is there a compliance program Yes ☒ No ☐

Explain

See Attachment A, URE-1 Disposition Document for Compliance Program.

Is senior management supportive Yes ☒ No ☐

Explain

See Attachment A, URE-1 Disposition Document for Compliance Program.

(4) Any attempt by the Registered Entity to conceal the violation or information needed to review, evaluate or investigate the violation

Yes ☐ No ☒

Explain

(5) Any evidence this was an intentional violation

Yes ☐ No ☒

Explain

(6) Any other extenuating circumstances

Yes ☐ No ☒