PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 28, 2011

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Disposition Documents attached hereto (Attachment a), 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 URE does not dispute the violations of CIP-004-2 R2 and CIP-006-1 R1/CIP-006-2 R2.2[3] and the assessed twelve thousand six hundred dollar ($12,600) penalty. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201002372 and WECC201002283 are Confirmed Violations, as that term is defined in the NERC Rules of Procedure and the CMEP.

[1] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.
[2] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).
[3] Reference to "CIP-006-1" refers to all versions of CIP-006. The CIP-006-1 violation covers July 1, 2009 through November 3, 2010. CIP-006-1 was in effect between July 1, 2009 and March 31, 2010. Version 2, CIP-006-2, was in effect between April 1, 2010 and September 30, 2010. CIP-006-3, Version 3, was effective October 1, 2010 through the remainder of the violation period.

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

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Statement of Findings Underlying the Violations

This NOP incorporates the findings and justifications reported in the Notice of Confirmed Violation and Proposed Penalty or Sanction (NOCV) issued on March 15, 2011, by Western Electricity Coordinating Council (WECC), as described in the Disposition Documents. 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 this NOP by the NERC Board of Trustees Compliance Committee (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 at issue in this NOP.

NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
NOC-845	WECC201002372	CIP-004-2	2	Medium	9/15/10-6/14/11	12,600
	WECC201002283	CIP-006-1	1	Medium[4]	7/1/09-10/22/10	

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

CIP-004-2 R2 - OVERVIEW

URE submitted a Self-Report to WECC. WECC determined that URE did not ensure that one individual out of 332 URE employees received Cyber Security Training prior to being granted access to Critical Cyber Assets. Two additional URE employees, after completing training during the previous year, did not complete Cyber Security "retraining" within a 365 day interval.

CIP-006-1 R1 - OVERVIEW

URE submitted three Self-Reports to WECC. WECC determined that URE did not identify a secured and monitored doorway as a Physical Security Perimeter access point pursuant to R1.2. Also, URE' Physical Security Plan failed to adequately address two of 27 protective measures implemented with respect to ten Cyber Assets used in physical access control and monitoring pursuant to R1.8. Specifically, URE did not implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events, the security monitoring controls did not issue automated or manual alerts for detected Cyber Security Incidents, and URE did not review logs of system events related to cyber security and maintain records documenting review of logs.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance

[4] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; R1.7 and R1.8 each have a "Lower" VRF.
[5] *See* 18 C.F.R § 39.7(d)(4).

Orders,[6] the NERC BOTCC reviewed the NOCV and supporting documentation on June 10, 2011. The NERC BOTCC approved the NOCV and the assessment of a twelve thousand six hundred dollar ($12,600) financial penalty against URE based upon WECC's findings and determinations, the NERC BOTCC's review of the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. the violations constituted URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE self-reported the violations;
3. WECC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which WECC considered a mitigating factor, as discussed in the Disposition Documents;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), as discussed in the Disposition Documents; and
7. WECC 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 believes that the assessed penalty of twelve thousand six hundred dollars ($12,600) 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 the Commission, or, if the Commission decides to review the penalty, upon final determination by the Commission.

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

[6] *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).

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) Disposition Document for Common Information, included as Attachment a;
    a. Disposition Document for CIP-004-2 R2, included as Attachment a-1; and
    b. Disposition Document for CIP-006-1 R1, included as Attachment a-2.
b) URE's Response to the Notice of Alleged Violation and Proposed Penalty or Sanction included as Attachment b;
c) URE's Source Document for CIP-004-2 R2, included as Attachment c;
d) URE's Source Documents for CIP-006-1 R1, included as Attachment d;
e) URE's Revised Mitigation Plan MIT-10-3335 for CIP-004-2 R2, included as Attachment e;
f) URE's Revised Mitigation Plan MIT-09-3075for CIP-006-1 R1, included as Attachment f;
g) URE's Certification of Mitigation Plan Completion for CIP-004-2 R2, included as Attachment g; and
h) URE's Certification of Mitigation Plan Completion for CIP-006-1 R1, included as Attachment h; and
i) WECC's Verification of Mitigation Plan Completion for CIP-004-2 R2, included as Attachment i.
j) WECC's Verification of Mitigation Plan Completion for CIP-006-1 R1, included as Attachment j.

A Form of Notice Suitable for Publication[7]

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

[7] *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 Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 213-2673 (801) 582-3918 – facsimile Mark@wecc.biz Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6855 (801) 883-6894 – facsimile CWhite@wecc.biz Sandy Mooy* Associate General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7658 (801) 883-6894 – facsimile SMooy@wecc.biz	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 Christopher Luras* Manager of Compliance Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this 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
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment a

Disposition Document for Common Information

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment a

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS

Dated June 10, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-845**

REGIONAL ENTITY

Western Electricity Coordinating Council (WECC)

IS THERE A SETTLEMENT AGREEMENT YES ☐ NO ☒

WITH RESPECT TO THE VIOLATION(S), REGISTERED ENTITY

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

WITH RESPECT TO THE ASSESSED PENALTY OR SANCTION, REGISTERED ENTITY

ACCEPTS IT/ DOES NOT CONTEST IT YES ☒

I. PENALTY INFORMATION

TOTAL ASSESSED PENALTY OR SANCTION OF **$12,600** FOR **TWO** VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

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

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ NO ☐ UNDETERMINED ☐
EXPLAIN
URE had a documented compliance program in place at the time of the violation that WECC considered a mitigating factor in determining the penalty.

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

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

YES ☐ NO ☒
IF YES, EXPLAIN

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

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

NOTICE OF ALLEGED VIOLATION AND PROPOSED PENALTY OR SANCTION ISSUED
DATE: **2/8/11** OR N/A ☐

SETTLEMENT REQUEST DATE
DATE: OR N/A ☒

NOTICE OF CONFIRMED VIOLATION ISSUED
DATE: **3/15/11** OR N/A ☐

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

REGISTERED ENTITY RESPONSE CONTESTED
FINDINGS ☐ PENALTY ☐ BOTH ☐ DID NOT CONTEST ☒
HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-2 R2

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

DISPOSITION OF VIOLATION
Dated June 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002372	**WECC2010-610672**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-2	**2**		**Medium**	**Lower**

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

The purpose statement of CIP-004-2 provides in pertinent part: "Standard CIP-004-2 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness."

CIP-004-2 R2 provides:

> **R2. Training — The Responsible Entity[1] shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.**
>
> > **R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.**
> >
> > **R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following**

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

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.)

VIOLATION DESCRIPTION

URE submitted a Self-Report after it discovered that one individual had received authorized physical access privileges to Critical Cyber Assets (CCAs) prior to that individual completing mandatory Cyber Security Training. This individual had access to a single Physical Security Perimeter (PSP) containing CCAs without the training between September 15, 2010 and October 4, 2010. The WECC Subject Matter Expert (SME) determined that despite being granted authorized physical access rights to Critical Cyber Assets, the employee was not granted authorized cyber access. The grant of access spanned a total of nineteen days.

After submitting the Self-Report, URE discovered two additional instances of CIP-004-2 noncompliance. Two personnel did not complete Cyber Security "retraining" at least annually, URE explicitly defines annual as a "365 day interval." After this discovery, URE immediately reviewed access logs and over 3,700 physical access requests. URE provided evidence demonstrating that out of 332 URE employees with authorized access between July 1, 2009 and December 12, 2010, there was only one instance in which an employee was granted authorized access prior to completing cyber security training and only two URE employees, having completed training during the previous year, failed to complete retraining for 2010 within a 365 day interval.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although URE's Security Training Program did not ensure that the single employee completed training prior to being given authorized access privileges to CCAs, the employee had completed some cyber security training and a personnel risk assessment. URE provided evidence that demonstrated that despite receiving access privileges, the employee did not gain access or attempt to gain access to CCAs. The remaining two URE employees had completed cyber security training during the previous year.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) **9/15/10 (when the individual employee was granted authorized physical access privileges to CCAs prior to completing mandatory Cyber Security Training) through 6/14/11 (Mitigation Plan Completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **Self-Report**

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-3335**
DATE SUBMITTED TO REGIONAL ENTITY	**3/1/11**
DATE ACCEPTED BY REGIONAL ENTITY	**6/6/11**
DATE APPROVED BY NERC	**7/8/11**
DATE PROVIDED TO FERC	**7/13/11**

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

On December 30, 2010, URE submitted a Mitigation Plan. WECC reviewed the Mitigation Plan and determined that URE mitigated the immediate risk of noncompliance on October 4, 2010. WECC issued acceptance for URE's Mitigation Plan on January 18, 2011. On March 1, 2011 URE submitted a Revised Mitigation Plan that included revisions to address the additional two instances in which employees with authorized access to CCAs did not complete Annual Cyber Security refresher training within 365 days. URE revised its Mitigation Plan to include policy revisions and extending the completion date to July 1, 2011.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**10/4/10**
EXTENSIONS GRANTED	**7/1/11**
ACTUAL COMPLETION DATE	**6/14/11**
DATE OF CERTIFICATION LETTER	**6/14/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**6/14/11**
DATE OF VERIFICATION LETTER	**7/27/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**6/14/11**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

1. **URE issued guidance to staff charged with validating training completion to avoid similar mistakes in the future**
2. **URE reviewed all other access requests and training records to ensure that this was the only instance of noncompliance**
3. **URE restructured its IT department**
4. **URE explored and evaluated potential for automated integration between access authorization system and the training records system to streamline access authorizations going forward**
5. **URE made changes to its training system in cooperation with the training application vendor**
6. **URE completed a redesign of its access request system**

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

1. **URE Security Awareness training program documentation**
2. **URE annual retraining program documentation**
3. **URE Security Awareness training completion logs/completion**
4. **Training completion and Access review process**

5. **Attestations from Training Personnel**
6. **Attestations from security personnel who review records to ensure personnel with access have completed training and annual retraining.**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-004-2 R2

MITIGATION PLAN
URE's Revised Mitigation Plan MIT-10-3335 for CIP-004-2 R2

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-004-2 R2

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion for CIP-004-2 R2

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-006-1 R1

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment a-2

DISPOSITION OF VIOLATION

Dated June 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002283	**WECC2010-610387**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-006-1[1]	**1**		**Medium**[2]	**N/A**[3]

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

The purpose statement of CIP-006-1 provides in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R1 provides:

> **R1. Physical Security Plan — The Responsible Entity[4] shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:**
>
> > **R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative**

[1] Reference to "CIP-006-1" refers to all versions of CIP-006. The CIP-006-1 violation covers July 1, 2009 through November 3, 2010. CIP-006-1 was in effect between July 1, 2009 and March 31, 2010. Version 2, CIP-006-2, was in effect between April 1, 2010 and September 30, 2010. CIP-006-3, Version 3, was effective October 1, 2010 through the remainder of the violation period.

[2] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; R1.7 and R1.8 each have a "Lower" VRF.

[3] At the time of the violations, no VSLs were in effect for CIP-006-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[4] Within the text of Standard CIP-006, "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.

measures to control physical access to the Critical Cyber Assets.

R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

(Footnote added.)

VIOLATION DESCRIPTION

URE submitted three Self-Reports to WECC. The first Self-Report submitted by URE cited a failure to secure Cyber Assets associated with Physical Security

Perimeter (PSP) access control and monitoring pursuant to R1.8. This Self-Report opened WECC's review of URE's compliance with CIP-006-1 R1. During implementation of mitigation activities for the R1.8 violation, URE discovered that it failed to identify PSP access points pursuant to R1.2, and submitted a second Self-Report. The WECC Subject Matter Expert (SME) determined that the second Self-Report did not constitute a separate violation outside the scope of the open R1 violation, and therefore expanded the scope of WECC's CIP-006-1 R1 investigation to include all sub-requirements, with particular emphasis on R1.2 and R1.8.[5]

URE submitted a third Self-Report which cited a failure to secure a Cyber Asset pursuant to CIP-006-2 R2.2.[6] Given the procedural history of CIP-006-1 R1.8 and CIP-006-2 R2.2, and based on the facts disclosed by URE, WECC Enforcement determined URE's Self-Reports citing violations of both R1.8 and R2.2 constituted a single violation. URE's noncompliance with R1.8 was limited to a total of nine Cyber Assets and URE' noncompliance with R2.2 was limited to a total of one Cyber Asset. Therefore there were a total of ten Cyber Assets that were afforded twenty-five out of a total of twenty-seven applicable security measures prescribed under CIP-006-1 R1.8. Specifically, URE did not implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events, the security monitoring controls did not issue automated or manual alerts for detected Cyber Security Incidents, and URE did not review logs of system events related to cyber security and maintain records documenting review of logs.

The WECC SMEs completed their review of URE noncompliance and determined that URE was in violation of CIP-006-1 R1 because it did not identify a secured and monitored doorway as a PSP access point pursuant to R1.2. Also, URE's Physical Security Plan failed to adequately address protective measures implemented with respect to ten Cyber Assets used in physical access control and monitoring.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because risks from R1.2 were limited by on-site security measures which were in place at the unidentified access point. The access point was permanently locked, and only a handful of identified security personnel with proper credentialing were granted

[5] WECC issued formal notice of its rejection of the URE's second Self-Report.
[6] CIP-006-1 R1.8 was in effect between July 1, 2009 and March 31, 2010. The second version of CIP-006, CIP-006-2 became effective as of April 1, 2010 and remunerated CIP-006-1 R1.8 as CIP-006-2 R2.2. WECC determined the violations of CIP-006-1 R1.8 and CIP-006-2 R2.2 are, therefore, identical in that compliance thereto requires entities to afford Cyber Assets protective measures. CIP-006-2 R2.2 states "… Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2."

access rights. Further, any ingress or egress through the access point was rendered virtually impossible by a large bookcase installed directly in front of the access point. The noncompliance with R1.8 did not result in any unauthorized physical or cyber access to Critical Cyber Assets or Cyber Assets, and URE provided evidence that the Cyber Assets were located in ESPs and physically secured from malicious attack or misuse.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) **7/1/09 through 10/22/10 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **Self-Report**

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-3075**
DATE SUBMITTED TO REGIONAL ENTITY	**1/31/11**
DATE ACCEPTED BY REGIONAL ENTITY	**4/21/11**
DATE APPROVED BY NERC	**5/18/11**
DATE PROVIDED TO FERC	**5/18/11**

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

On August 26, 2010, URE submitted its Mitigation Plan addressing the R1.8 violation. WECC reviewed the Mitigation Plan on November 5, 2010 and issued a notice of Mitigation Plan acceptance on November 8, 2010. Further review of URE noncompliance expanded the scope of the violation initially reported and mitigated

by URE. WECC issued a notice of Mitigation Plan rejection on January 25, 2011 and requested URE submit a revised Mitigation Plan that addressed the full scope of noncompliance. On January 31, 2011, URE submitted a revised Mitigation Plan.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**10/22/10**
DATE OF CERTIFICATION LETTER	**4/21/11**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**10/22/10**
DATE OF VERIFICATION LETTER	**4/26/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**10/22/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE has completed the following steps in order to mitigate R1.2 and R1.8 violations:

1. **All historical logs for these Cyber Assets have been reviewed and no evidence of a cyber incident was found during this review.**
2. **URE immediately incorporated these devices into the procedure used for monitoring security events on other Cyber Assets.**
3. **URE reviewed the complete list of Cyber Assets in the categories of Critical Cyber Assets, Associated Cyber Assets and Assets used in access control and monitoring in order to ensure that no other Cyber Assets had been missed.**
4. **Documentation has been completed to institutionalize these changes, and the new procedure has been communicated to affected parties.**
5. **All monitoring of the affected devices has been moved in order to automate this work.**
6. **When URE re-evaluated its interpretation of what it considered a 'PSP Access Point', URE immediately posted a guard at the door and then proceeded to have the door lock mechanism made inoperable.**
7. **URE removed the door and dry-walled in the space.**
8. **URE made a change to its URE CIP Physical Security Plan to add a formal definition of 'PSP Access Point.'**
9. **URE retroactively applied its complete change management process to the physical access control system panel, including completing the documentation required by URE's process as well as a complete new Cyber Asset security controls test.**
10. **URE subsequently completed all other documentation updates necessitated by this change. URE altered its CIP change control**

procedure to require additional steps and safeguards for new additions of cyber assets.

11. **URE conducted additional training for the groups responsible for such changes.**

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

- **All historical logs for these Cyber Assets**
- **A complete list of Cyber Assets in the categories of Critical Cyber Assets**
- **Associated Cyber Assets and Assets used in access control and monitoring**
- **Various correspondence and data requests between URE and WECC Enforcement Staff**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-006-1 R1

MITIGATION PLAN
URE's Revised Mitigation Plan MIT -09-3075 for CIP-006-1 R1 s

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-006-1 R1

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Mitigation Plan Completion for CIP-006-1 R1