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 Settlement Agreement (Attachment a) and the Disposition Documents (Attachment b), 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 Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations of CIP-006-1 Requirement (R)1, and CIP-007-1 R2, R4, and R5. According to the Settlement Agreement, stipulates to the facts of the violations, and has agreed to the assessed penalty of eighteen thousand dollars ($18,000), 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 WECC201002230, WECC201002232, WECC201002233, WECC201002234 are being filed in accordance with 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).

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

Statement of Findings Underlying the Violations

This NOP incorporates the findings and justifications set forth in the Settlement Agreement executed on May 6, 2011, by and between WECC and URE. The details of the findings and the basis for the penalty are set forth in the Disposition Documents. This NOP filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7, NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
NOC-880	WECC201002230	CIP-006-1	1.1	Medium[3]	1/1/10 - 3/30/10	18,000
	WECC201002232	CIP-007-1	2	Medium	1/1/10 - 6/30/10	
	WECC201002233		4	Lower		
	WECC201002234		5	Medium		

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

CIP-006-1 R1- OVERVIEW

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process in which URE was required to self-certify its compliance with CIP-002 through CIP-009. URE submitted a Self-Report citing possible noncompliance with CIP-006-1 R1. URE subsequently submitted its Self-Certification citing noncompliance as described in the Self-Report.[4] WECC determined that URE violated CIP-006-1 R1 by failing to implement its Physical Security Plan and ensure that all Critical Cyber Assets were within a Physical Security Perimeter at its facility.

CIP-007-1 R2, R4 and R5 - OVERVIEW

The Self-Report also cited noncompliance with CIP-007-1 R2, R4, and R5. The Self-Certification cited noncompliance as described in the Self-Report.[5] The scope of the violations extends to Cyber Assets associated with two Critical Assets, the facility and Control Center. WECC determined that, due to departure of IT staff, URE did not ensure only ports and services required for normal and emergency operations were enabled, failed to document and implement anti-virus and malware prevention tools, failed to document compensating measures applied to mitigate risks posed by the absence of anti-virus and malware prevention tools and their implementation, and failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for all user activity.

[3] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; R1.7, R1.8 and R1.9 each have a "Lower" VRF.
[4] Because URE submitted its Self-Report during the Self-Certification submission period, the discovery method for this violation is classified as Self-Certification.
[5] The discovery method for this violation was also considered Self-Certification.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[6]

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,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation July 11, 2011. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of an eighteen thousand dollar ($18,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. the violations constituted URE's first occurrence of violation of the subject NERC Reliability Standards;
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 approved the Settlement Agreement and believes that the assessed penalty of eighteen thousand dollars ($18,000) 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.

---

[6] *See* 18 C.F.R. § 39.7(d)(4).

[7] *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).

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 part of this NOP are the following documents:

a) Settlement Agreement by and between WECC and URE executed May 6, 2011, included as Attachment a;

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

   i. Disposition Document for CIP-006-1 R1, included as Attachment b.1;

   ii. Disposition Document for CIP-007-1 R2, R4, and R5, included as Attachment b.2;

c) URE's Self-Certification for of CIP-006-1 R1, CIP-007-1 R2, R4, and R5, included as Attachment b;[8]

d) URE's Mitigation Plan MIT-10-2960 for CIP-006-1 R1, included as Attachment c;

e) URE's Revised Mitigation Plan MIT-10-2960 for CIP-006-1 R1, included as Attachment d;

f) URE's Mitigation Plan MIT-10-2977 for CIP-007-1 R2, R4, and R5, included as Attachment e;

g) Certification of Mitigation Plan Completion for CIP-006-1 R1, included as Attachment f;

h) Certification of Mitigation Plan Completion for CIP-007-1 R2, R4, and R5, included as Attachment f;

i) WECC's Verification of Certification of Mitigation Plan Completion for CIP-006-1 R1 , included as Attachment g; and

j) WECC's Verification of Certification of Mitigation Plan Completion for CIP-007-1 R2, R4, and R5, included as Attachment h.

[8] The Self-Certification references a violation of CIP-006-1 R4 which was later dismissed by WECC.

A Form of Notice Suitable for Publication[9]

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

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 Davis Smith* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net davis.smith@nerc.net 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.

[9] *See* 18 C.F.R. § 39.7(d)(6).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

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

Respectfully submitted,

/s/ *Rebecca J. Michael*

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

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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment b

Disposition Document for Common Information

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment b

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS

Dated July 11, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity(URE)	**NCRXXXXX**	**NOC-880**

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 ☒
Agrees to the stipulated facts
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 **$18,000** FOR **FOUR** 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
WECC reviewed URE's Internal Compliance Program (ICP) and considered it 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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

(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: **1/4/11** OR N/A ☐

SETTLEMENT REQUEST DATE
DATE: **1/14/11** OR N/A ☐

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

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

REGISTERED ENTITY RESPONSE CONTESTED
FINDINGS ☐ PENALTY ☒ BOTH ☐ DID NOT CONTEST ☐

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

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 b-1

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002230	**WECC2010-610061**

I. VIOLATION INFORMATION

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

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

The purpose statement of CIP-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 R1.1 provides:

> **R1. Physical Security Plan — The Responsible Entity[3] 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 measures to control physical access to the Critical Cyber Assets.**

Footnote added.

[1] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; R1.7, R1.8 and R1.9 each have a "Lower" VRF.
[2] At the time of the violation, 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.
[3] 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.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

VIOLATION DESCRIPTION

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process in which URE was required to self-certify its compliance with CIP-002 through CIP-009. URE submitted a Self-Report citing possible noncompliance with CIP-006-1 R1. URE subsequently submitted its Self-Certification citing noncompliance as described in the Self-Report. The discovery method for this violation is classified as Self-Certification because URE submitted its Self-Report during the Self-Certification submission period.

URE reported noncompliance with CIP-006-1 R1 because it failed to secure all Critical Cyber Assets (CCAs) within an identified "six-walled" Physical Security Perimeter (PSP) by December 31, 2009. URE reported that the scope of its noncompliance extended to CCAs at three locations, a facility, a Control Center, and another location housing servers.

A WECC Subject Matter Expert (SME) reviewed URE's Self-Report. The SME determined that URE was in possible violation of CIP-006-1 R1 because CCAs associated with Critical Assets at a facility and Control Center were not secured within a PSP. Specifically, the SME cited URE's failure to complete construction removing the dropped ceiling at the facility housing CCAs. The CCAs located within two identified PSPs were enclosed in a completely enclosed ("six-wall") border as required under CIP-006-1 Requirement 1.1. One PSP boarder was a drop ceiling, with commercial-grade acoustic ceiling tile and fluorescent light fixtures, is installed below the structural ceiling. As a result, there was a space through which a person could theoretically gain access. Further, the SME found that URE did not complete construction at a second PSP. The SME, therefore, determined that URE violated CIP-006-1 R1.1 and forwarded his findings to WECC Enforcement.

WECC Enforcement reviewed URE's Self-Report and the SME's determination. Although WECC Enforcement determined that URE failed to secure CCAs within a PSP at the facility in violation of CIP-006-1 R1.1, WECC Enforcement determined that the scope of URE's violation did not extend to CCAs within a PSP at two locations.[4]

[4] WECC Enforcement investigated URE's Self-Report regarding the Control Center and another location and WECC later determined that URE did not violate CIP-006-1 R1 with respect to CCAs within PSPs as the facility under construction that was brought online only after the PSP was constructed.

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

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because compensating measures were implemented by URE. URE staffed the Physical Security Perimeter with security staff to ensure that CCAs were not accessed without authorization. In addition, although CCAs were not secured within a PSP as required by the standard, URE demonstrated that facilities were equipped with badge readers and 24/7 onsite security personnel to control and monitor escorted access onsite.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT	☐
SELF-CERTIFICATION[5]	☒
COMPLIANCE AUDIT	☐
COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK	☐
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

DURATION DATE(S): **1/1/10 through 3/30/10 (PSP construction at the facility control room was completed)**

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

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 ☒

[5] Although the Settlement Agreement indicates that this violation was self-reported during a self-certification period, in assessing the penalty, WECC gave URE full credit for self-reporting. URE provided evidence, after the Notice of Alleged Violation and Penalty or Sanction was issued, that it had attempted to self-report this violation prior to the self-certification period.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2960**
DATE SUBMITTED TO REGIONAL ENTITY	**3/26/10**
DATE ACCEPTED BY REGIONAL ENTITY	**10/13/10**
DATE APPROVED BY NERC	**11/5/10**
DATE PROVIDED TO FERC	**11/5/10**

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

On January 4, 2010, URE submitted its Mitigation Plan. On March 26, 2010 URE submitted an Extension Request and Revised Mitigation Plan with a new completion date of May 20, 2010, referencing delays in reaching an agreement regarding exclusive control of electronic access monitoring devices with another location owner. Although the Mitigation Plan completion was extended, construction activities at the facility and Control Center proceeded on schedule, completing on March 30, 2010.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**3/30/10**
	EXTENSIONS GRANTED **Yes**
ACTUAL COMPLETION DATE	**5/20/10**
DATE OF CERTIFICATION LETTER	**5/20/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**5/20/10**
DATE OF VERIFICATION LETTER	**10/27/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**5/10/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE developed and implemented a Physical Security Plan to ensure all CCAs were located within PSPs and completed construction at the facility and Control Center in compliance with CIP-006-1 R1.1. URE also eliminated the "dropped" ceiling in the PSP and implemented its Physical Security Plan to ensure that all CCAs were located within PSPs. In addition, URE reached agreement to maintain exclusive control of electronic access monitoring devices. Although WECC Enforcement determined that the scope of the violation extended only to these two PSPs, SMEs verified that all construction activities and mitigation measures were completed as prescribed by its Mitigation Plan.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

URE Physical Security Plan

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Certification

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2960 Submittal Form

URE's Revised Mitigation Plan MIT-10-2960 Submittal Form

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

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Certification of Mitigation Plan Completion

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007-1 R2, R4, and R5

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment b-2

DISPOSITION OF VIOLATION
Dated July 11, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002232	**WECC2010-610063**
WECC201002233	**WECC2010-610064**
WECC201002234	**WECC2010-610065**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	**2**		**Medium**	**N/A**[1]
	4		**Lower**	
	5		**Medium**	

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

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

> **Standard CIP-007 requires Responsible Entities[2] to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.**

Footnote added.

CIP-007-1 R2 provides:

> **R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.**

[1] At the time of the violations, no VSLs were in effect for CIP-007-1. 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.

[2] Within the text of Standard CIP-007, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R4 provides:

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

CIP-007-1 R5 provides:

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

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

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

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and “special” characters.

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

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

VIOLATION DESCRIPTION

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process in which URE was required to self-certify its compliance with CIP-002 through CIP-009. URE submitted a Self-Report citing possible noncompliance with CIP-007-1 R2, R4, and R5. URE subsequently submitted its Self-Certification citing noncompliance as described in the Self-Report. The discovery method for this violation is classified as Self-Certification because URE submitted its Self-Report during the Self-Certification submission period. The scope of the violations extends to Cyber Assets associated with two Critical Assets, a facility and a Control Center.

URE indicated that noncompliance of CIP-007-1 R2, R4, and R5 in this case was caused by the departure of a number of IT personnel overseeing CIP Compliance. Consequently, URE's CIP implementation was delayed. Although URE reported it had begun implementation of CIP-007-1 R2, it failed to ensure compliance by December 31, 2009. In addition, URE was in violation of CIP-007-1 R4 as it failed to document and implement anti-virus and malware prevention tools and failed to document compensating measures applied to mitigate risks posed by the absence of anti-virus and malware prevention tools and their implementation, by December 31, 2009. The lack of IT staff also led to URE's violation of CIP-007-1 R5. WECC Enforcement found that URE failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for all user activity related to the Cyber Assets at the facility and Control Center as prescribed by CIP-007-1 R5 by December 31, 2009.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed by noncompliance was, to an extent, lessened because the Cyber Assets associated with the two Critical Assets, a facility and Control Center, were within an Electronic Security Perimeter (ESP) and were afforded some measure of protection through tripwires and electronic access controls. WECC determined that URE's violation of CIP-007-1 R2 and R4 posed a minimal risk to the BPS, while URE's violation of CIP-007-1 R5 posed a moderate risk.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) **1/1/10 through 6/30/10 (Mitigation Plan completion)**

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

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-10-2977**
DATE SUBMITTED TO REGIONAL ENTITY	**1/4/10**
DATE ACCEPTED BY REGIONAL ENTITY	**10/13/10**
DATE APPROVED BY NERC	**11/8/10**
DATE PROVIDED TO FERC	**11/10/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

[3] Since URE submitted its Self Report prior to the certification period and prior to the compliance date, WECC gave URE full credit for self-reporting when assessing the penalty but because URE submitted its Self Report during the Self-Certification submission period, the discovery method is classified as Self-Certification.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

EXPECTED COMPLETION DATE	**6/30/10**
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	**6/30/10**
DATE OF CERTIFICATION LETTER	**6/30/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**6/30/10**
DATE OF VERIFICATION LETTER	**11/23/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**6/30/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE's Mitigation Plan identified the following steps to be completed by June 30, 2010:

1. Full deployment of Symantec Protection Suite, (Milestone March 30, 2010);
2. Completion of the DCS upgrade; and
3. Completion of mitigation action including:

a. Establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

b. Establish, Implement, and document technical and procedural controls that enforce access authentication of, and accountability for all user activity and that minimize the risk of unauthorized system access.

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

- **URE's Procedure for CIP-007 R2**
- **URE's Procedure for CIP-007 R4**
- **URE's Procedure for CIP 007 R5**
- **Ports and services scan report**
- **Screen shots of access logs for shared accounts**
- **Review of shared Accounts and access logs between (July 25, 2010 and October 25, 2010)**
- **Symantec Antivirus and Anti-software screenshot and scan results**
- **Lists of shared accounts**
- **List of users that have access to the shared accounts**
- **An explanation of the process of determining which personnel qualify for "need to know" access**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Certification form

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2977 Submittal Form

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

VERIFICATION BY REGIONAL ENTITY
WECC's Verification of Certification of Mitigation Plan Completion