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, 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-003-1 Requirement (R) 3, CIP-005-1 R2, CIP-006-1 R1 and CIP-007-1 R5. According to the Settlement Agreement, URE stipulates to the facts of the violations and has agreed to the assessed penalty of thirty seven thousand five hundred dollars ($37,500), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the

[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

Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC200901666, WECC200901690, WECC200901753 and WECC200901700 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 January 4, 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-771	WECC200901666	CIP-003-1	3	Lower	7/1/08 – 8/21/09	37,500
	WECC200901690	CIP-005-1	2	Medium[3]	7/1/09 – 10/15/09	
	WECC200901753	CIP-006-1	1	Medium[4]	7/1/09 – 4/9/10	
	WECC200901700	CIP-007-1	5	Lower	7/1/09 – 11/13/09	

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

CIP-003-1 R3 - OVERVIEW

As a result of a Self-Certification (Self-Certification),[5] WECC determined that URE did not document four instances where Cyber Assets could not conform to URE's Cyber Security policy, and did not document the instances as exceptions that had been authorized by the senior manager, as required by the standard.

CIP-005-1 R2 - OVERVIEW

As a result of a Self-Report (Self-Report), WECC determined that URE did not configure its Energy Management System's (EMS) firewalls within URE's Electronic Security Perimeter (ESP) to deny all access by default at network access points, as required by the standard.

[3] CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" VRF; R2.5 and its sub-requirements and R2.6 each have a "Lower" VRF.
[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, R1.8 and R1.9each have a "Lower" VRF.
[5] URE submitted a Self-Report for this violation. Nevertheless, because the Self-Report was submitted during a Self-Certification submittal period, WECC classified the discovery method as Self-Certification.

CIP-006-1 R1 - OVERVIEW

As a result of a Self-Certification,[6] WECC determined that URE did not address all sub-requirements of CIP-006-1 R1 in URE's Cyber Security Plan. Specifically, URE: (1) did not develop processes to ensure and document that all of its Cyber Assets within an ESP also resided within an identified Physical Security Perimeter (PSP); (2) did not develop processes for the identification of all access points through each PSP or develop measures to control entry at those access points; (3) did not develop processes, tools, and procedures for monitoring access at access points to each perimeter; (4) did not develop procedures for the appropriate use of physical access controls; (5) did not develop processes for updating URE's physical security plan; (6) did not develop processes for the access control and monitoring of the PSP; and (7) did not develop a process for conducting an annual review of URE's physical security plan, as required by the standard.

CIP-007-1 R5 - OVERVIEW

As a result of a Self-Report, WECC determined that URE did not use passwords on its EMS system that met requirements for password strength or for annual change, as required by the standard.

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 WECC's assessment of a thirty seven thousand five hundred dollar ($37,500) 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. WECC reported that URE was cooperative throughout the compliance enforcement process;
2. URE had a compliance program at the time of the violation which WECC considered a mitigating factor, as discussed in the Disposition Documents;

[6] URE submitted a Self-Report for this violation. Nevertheless, because the Self-Report was submitted during a Self-Certification submittal period, WECC classified the discovery method as Self-Certification.
[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).

3. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
4. WECC determined that the violations posed a minimal risk, except for CIP-006-1 R1 which posed a moderate 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
5. 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 thirty-seven thousand five hundred dollars ($37,500) 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 part of this NOP are the following documents:

a) Settlement Agreement by and between WECC and URE executed January 4, 2011, included as Attachment a;

b) Common Disposition Document, included as Attachment b;

   i. Disposition Document for CIP-003-1 R3, included as Attachment b-1;

   ii. Disposition Document for CIP-005-1 R2, included as Attachment b-2;

   iii. Disposition Document for CIP-006-1 R1, included as Attachment b-3; and

   iv. Disposition Document for CIP-007-1 R5, included as Attachment b-4.

c) Record Documents for CIP-003-1 R3:

   i. URE's Self-Certification, included as Attachment c-1;

   ii. URE's Mitigation Plan MIT-08-2039, included as Attachment c-2;

   iii. URE's Certification of Mitigation Plan Completion, included as Attachment c-3; and

   iv. WECC's Verification of Mitigation Plan Completion, included as Attachment c-4.

d) Record Documents for CIP-005-1 R2:

   i. URE's Self-Report, included as Attachment d-1;

   ii. URE's Revised Mitigation Plan MIT-09-2070, included as Attachment d-2;

   iii. URE's Certification of Mitigation Plan Completion, included as Attachment d-3; and

   iv. WECC's Verification of Mitigation Plan Completion, included as Attachment d-4.

e) Record Documents for CIP-006-1 R1:

   i. URE's Self-Certification, included as Attachment e-1;

   ii. URE's Mitigation Plan MIT-09-2180, included as Attachment e-2;

   iii. URE's Certification of Mitigation Plan Completion, included as Attachment e-3; and

   iv. WECC's Verification of Mitigation Plan Completion, included as Attachment e-4.

f) Record Documents for CIP-007-1 R5:

   i. URE's Self-Report, included as Attachment f-1;

   ii. URE's Revised Mitigation Plan MIT-09-2099, included as Attachment f-2;

   iii. URE's Certification of Mitigation Plan Completion, included as Attachment f-3; and

   iv. WECC's Verification of Mitigation Plan Completion, included as Attachment f-4.

A Form of Notice Suitable for Publication[9]
A copy of a notice suitable for publication is included in Attachment g.

[9] *See* 18 C.F.R. § 39.7(d)(6).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer David N. Cook* 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) 713-9598 (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.

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

Common Disposition Document

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

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS
Dated May 9, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-771**

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 ☒
Stipulates to the 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 **$37,500** 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
At the time of the violations, URE had an internal compliance program (ICP) 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: **12/22/09** OR N/A ☐

SETTLEMENT REQUEST DATE
DATE: **1/22/10** 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 ☒

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-003-1 R3

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

DISPOSITION OF VIOLATION
Dated May 9, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901666	**URE_WECC20091839**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-003-1	**3**		**Lower**	**N/A**[1]

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

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

CIP-003-1 R3 provides:

R3. Exceptions — Instances where the Responsible Entity[2] cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or

[1] At the time of the violations, no VSLs were in effect for CIP-003-1. 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-003, "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

delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

(Footnote added).

VIOLATION DESCRIPTION

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Report addressing its noncompliance with this standard and then approximately a week later, URE submitted its Compliance Certification Statement and reported the status of compliance for this standard as "Substantially Compliant." Although URE self-reported this violation, because it self-reported within the CIP Self-Certification submittal window, WECC classifies the discovery method for this violation as Self-Certification.

According to the Self-Report, URE conducted an internal evaluation in preparation for the Self-Certification process and discovered it had not documented exceptions in certain instances that did not conform to its Cyber Security policy. Under both URE's Cyber Security Policy and the referenced standard, URE was required to document any authorized exceptions to its Cyber Security policy within thirty days of being approved by URE's Senior Manager. WECC determined that URE granted four exceptions to its Cyber Security policy, but failed to document the senior manager's approval of those exceptions. The four exceptions pertained to: (1) passwords for service accounts on Unix/Linux devices; (2) limits on concurrent logins; (3) encryption of backups; and (4) password requirements and access logging for printers.

A WECC subject matter expert (SME) reviewed URE's Self-Report and Mitigation Plan, and found that URE had identified four instances where URE's Cyber Assets did not conform with all aspects of URE's Cyber Security policy, and the necessary exceptions to that policy were not documented and authorized by URE's senior manager or delegate(s). WECC's SME determined that URE had a violation of CIP-003-1 R3 for these four instances. WECC Enforcement confirmed these findings.

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 the four missing exceptions to URE's Cyber Security policy did not relate directly to security controls for Critical Cyber Assets. Although URE could not comply with certain aspects of its own internal security policy, in violation of the Standard, none of these exceptions reflected a deficiency in the security controls as required by the standard.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) **7/1/08 (date URE was required to be compliant with Standard) through 8/21/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **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-08-2039**
DATE SUBMITTED TO REGIONAL ENTITY	**7/10/09**
DATE ACCEPTED BY REGIONAL ENTITY	**10/6/09**
DATE APPROVED BY NERC	**10/20/09**
DATE PROVIDED TO FERC	**10/20/09**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**8/31/09**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**8/21/09**
DATE OF CERTIFICATION LETTER	**8/21/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**8/21/09**

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

DATE OF VERIFICATION LETTER **11/9/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **8/21/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

- **URE's director of Cyber Security reviewed each of the four instances where Cyber Assets could not conform to URE's Cyber Security policy and determined that the exceptions were necessary and appropriate.**

- **Each business unit of URE responsible for maintaining NERC-applicable Cyber Assets reviewed URE's Cyber Security policy and attested that the equipment was compliant with the requirements of the policy, or that an exception had been granted where necessary.**

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)

- **Memorandum from URE's director of Cyber Security**
- **URE's document delegating the CIP senior manager**
- **URE's Cyber Security and controls exception request form.**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Certification

MITIGATION PLAN
URE's Mitigation Plan MIT-08-2039

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-005-1 R2

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

DISPOSITION OF VIOLATION
Dated May 9, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901690	**URE_WECC20091864**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-005-1	**2**		**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-005-1 provides, in pertinent part: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."

CIP-005-1 R2 provides:

R2. Electronic Access Controls — The Responsible Entity[3] shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document,

[1] CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" VRF; R2.5 and its sub-requirements and R2.6 each have a "Lower" VRF.
[2] At the time of the violations, no VSLs were in effect for CIP-005-1. 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-005, "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

individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

(Footnote added).

VIOLATION DESCRIPTION

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process. URE reported a violation of the referenced standard through its Mitigation Plan addressing its noncompliance and approximately a week later, URE submitted its Compliance Certification Statement and reported its status of compliance for this Standard as "Substantially Compliant."

URE followed its Self-Certification submittal with a Self-Report. According to the Self-Report, URE has access lists on the Energy Management System (EMS) firewalls that are configured to allow specific networks to communicate with other networks using any port. Therefore, URE failed to implement deny-by-default access controls at the Electronic Security Perimeters (ESP) of its EMS.

A WECC subject matter expert (SME) reviewed URE's Self-Report and Mitigation Plan and determined that some access control list entries at access points to URE's ESP were not configured to deny all access by default. WECC's SME determined that URE failed to use an access control model which denies access by default, and that some firewall interfaces were configured with an access control list permitting

IP traffic from any host to any host (IP-any-any rule),[4] which allows unrestricted access through those interfaces, resulting in a violation of CIP-005-1 R2. WECC Enforcement reviewed the supporting documents and confirmed the findings of the WECC SME.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the violation posed a minimal risk and did not pose a serious of substantial risk to the reliability of the bulk power system (BPS) because URE's "IP-any-any" rule only applies to access between the two ESPs or either of the ESPs and the quality assurance network. The "IP-any-any" rule did not allow ingress to or egress from URE's corporate network, field data acquisition network segments, or the Internet. In addition, communications with other utilities and WECC were restricted by IP address and port at the URE LAN network at the corporate network level.

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 (date URE was required to be complaint with the Standard) through 10/15/09 (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	☒

[4] "IP-any-any" describes the process wherein URE has access lists on its EMS' firewalls that were configured to allow specific networks to communicate with other networks using any port and did not deny access by default.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2070**
DATE SUBMITTED TO REGIONAL ENTITY	**9/25/09**
DATE ACCEPTED BY REGIONAL ENTITY	**10/20/09**
DATE APPROVED BY NERC	**10/27/09**
DATE PROVIDED TO FERC	**10/28/09**

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

URE originally submitted this Mitigation Plan on June 30, 2009, which encompassed both power scheduling system and EMS. URE revised the Mitigation Plan to remove power scheduling system from the scope of the Mitigation Plan because URE determined that its power scheduling system is not essential to the operation of its System Control Center, and therefore, power scheduling system is no longer properly classified as a CCA.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**10/15/09**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**10/15/09**
DATE OF CERTIFICATION LETTER	**10/15/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**10/15/09**
DATE OF VERIFICATION LETTER	**11/20/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**10/15/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

- **URE reviewed the EMS Firewall assessment that was completed by IT Security.**
- **URE reviewed access lists on the System Control Center and Backup Control Center's respective EMS firewalls.**
- **URE determined what ports are required and the associated IP addresses for the firewall.**
- **URE rewrote the access lists for both EMS firewalls and get change control approval.**
- **URE tested the updated access lists.**

- **URE's IT Security re-ran the EMS firewall assessment to determine whether the problem was fixed correctly.**

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 mitigation plan results for the Critical Infrastructure Protection Cyber vulnerability**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report

MITIGATION PLAN
URE's Revised Mitigation Plan MIT-09-2070

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

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

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-3

DISPOSITION OF VIOLATION
Dated May 9, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901753	**URE_WECC20091944**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-006-1	**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 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.

[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 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.
[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.

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

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Report addressing its noncompliance with this Standard and approximately a week later, URE submitted its Compliance Certification Statement and reported the status of compliance for this standard as "Substantially Compliant." Although URE self-reported this violation, because it

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

self-reported within the CIP Self-Certification submittal window, WECC classified the discovery method for this violation as Self-Certification. According to the Self-Report, URE conducted an internal evaluation in preparation for the self-certification process, and discovered that its Physical Security Plan did not address all the sub-requirements of R1 of the Standard.

A WECC subject matter expert (SME) reviewed the Self-Report and the Mitigation Plan to confirm that URE's Physical Security Plan did not address all of the sub-requirements of ClP-006-1 R1. WECC's SME determined that URE's Corporate Security department used an electronic access control system that was provided and serviced by a third-party vendor. In addition, URE's Information Technology (IT) department had not provided any support to the Corporate Security department for the cyber assets used in the access control and monitoring of the Physical Security Perimeter.

WECC's SME determined that URE was in violation of multiple sub-requirements of the standard, including those related to containing Critical Cyber Assets within a "six-wall" border (R1.1); identification of physical perimeter access points and control of access through such points (R1.2); processes, tools, and procedures for monitoring access at access points (R1.3); procedures for the appropriate use of physical access controls (R1.4); processes for updating URE's physical security plan (R1.7); procedures for the access, control and monitoring of the Physical Security Perimeter(s) (R1.8); and annual reviews of URE's physical security plan (R1.9). Because URE was not able to address the sub-requirements of R1 of the Standard, the SME determined URE was in violation of ClP-006-1 R1. WECC Enforcement reviewed the supporting documents and confirmed the SME's findings.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

WECC determined that the violation posed a moderate risk to the reliability of the bulk power system (BPS) because the failure to develop processes for protecting and monitoring access points to URE's Cyber Assets could compromise the operations or physical integrity of URE's Cyber Assets, which could possible cause a widespread negative impact to the BPS. WECC did, however, determine that the violation did not pose a serious or substantial risk the reliability of the BPS because URE had a document, that, although not specific to the requirements of CIP-006-1 R1, did identify measures to protect company assets, security systems, etc.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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 (date URE was required to be compliant with Standard) through 4/9/10 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **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-09-2180**
DATE SUBMITTED TO REGIONAL ENTITY	**7/10/09**
DATE ACCEPTED BY REGIONAL ENTITY	**12/8/09**
DATE APPROVED BY NERC	**12/18/09**
DATE PROVIDED TO FERC	**12/18/09**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**4/9/10**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**4/9/10**

DATE OF CERTIFICATION LETTER **4/9/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **4/9/10**

DATE OF VERIFICATION LETTER **6/8/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **4/9/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

- **URE completed all written policies and procedures to establish compliance with all sub-requirements of CIP-006-1 R1.**

- **URE completed scoping of all technical changes needed to Corporate Security operations to comply with the written policies and procedures.**

- **URE completed testing and implementation of all technical 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)

- **URE's CIP-006 R1 Mitigation Plan evidence**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Certification

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2180

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007-1 R5

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION
Attachment b-4

DISPOSITION OF VIOLATION
Dated May 9, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC200901700	**URE_WECC20091874**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	**5**	**5.3**	**Lower**	**N/A**[1]

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

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

> **R5. Account Management — The Responsible Entity[2] 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.**
>
> **R5.3. 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.**

[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.

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

VIOLATION DESCRIPTION

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process. URE reported a violation of the Standard through its Mitigation Plan submittal and approximately a week later, URE submitted its Compliance Certification Statement and reported its status of compliance for this Standard as "Substantially Compliant." URE followed its Self-Certification submittal with a Self-Report.

According to the Self-Report, URE has service accounts on its Energy Management System (EMS) that use passwords that do not meet the requirements of R5.3 of the Standard for password strength or for annual change. URE determined that it was not able to bring these accounts into compliance with the Standard by the July 1, 2009 compliance date.

A WECC subject matter expert (SME) conducted an interview with URE personnel to confirm that the accounts in question relate to URE's EMS application, including a network management protocol services associated with it. The WECC SME reviewed the Self-Report, the revised Mitigation Plan and the interview responses and confirmed that password requirements for certain system accounts did not meet the requirements of the Standard for annual changes or password complexity by July 1, 2009. WECC Enforcement reviewed the supporting documents and confirmed that URE was in violation of CIP-007-1 R5.

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 the accounts in question were used within a monitored system internal to URE's EMS system and were only accessible from within the ESP.

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 (date URE was required to be compliant with Standard) through 11/13/09 (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-09-2099**
DATE SUBMITTED TO REGIONAL ENTITY	**9/15/09**
DATE ACCEPTED BY REGIONAL ENTITY	**10/23/09**
DATE APPROVED BY NERC	**11/23/09**
DATE PROVIDED TO FERC	**11/24/09**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE
URE originally submitted a Mitigation Plan for this violation on June 30, 2009. On September 15, 2009, URE submitted a revised Mitigation Plan due to changes related to URE's violation of CIP-005-1 R2 (WECC200901690).

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**11/15/09**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**11/13/09**
DATE OF CERTIFICATION LETTER	**11/13/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**11/13/09**
DATE OF VERIFICATION LETTER	**5/26/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**11/13/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

- **URE identified all instances where source code needed to be modified to update passwords on service accounts.**

- **URE developed a process to update the passwords on service accounts and test that process in a test environment.**

- **URE implemented the process to update passwords on service accounts and created a list of service accounts subject to this requirement to allow for the passwords to be updated.**

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)

- **Mitigation Plan Completion form**
- **Technical Feasibility Exception request**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report

MITIGATION PLAN
URE's Revised Mitigation Plan MIT-09-2099

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

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