PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 26, 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 (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-004-1 Requirement (R) 4, CIP-005-1 R1.5 and CIP-006-2 R1 and the assessed twelve thousand two hundred dollar ($12,200) penalty. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201002154, WECC201002236 and WECC201002152 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).

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 set forth in the Notice of Confirmed Violation and Proposed Penalty or Sanction (NOCV) issued on December 17, 2010, by the Western Electricity Coordinating Council (WECC). 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-755	WECC201002154	CIP-004-1	4.1, 4.2	Medium[3]	7/01/09 – 7/12/10[4]	12,200
	WECC201002236	CIP-005-1[5]	1/1.5	Medium[6]	7/01/09– 6/30/10	
	WECC201002152	CIP-006-2[7]	1	Medium	7/01/09 – 8/17/10	

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

CIP-004-1 R4.1 and 4.2 - OVERVIEW

As a result of a Self-Report, WECC determined that URE did not revoke an employee's authorized unescorted physical access to Critical Cyber Assets (CCAs) until May 5, 2010. Access should have been revoked no later than September 18, 2009 in accordance with the standard.

CIP-005-1 R1.5 - OVERVIEW

As a result of a Self-Report, WECC determined that URE did not ensure protective measures to URE's CCAs because an URE employee performed an escort function on June 4, 2010 without a valid personnel risk assessment (PRA). Therefore, URE did not follow its own PRA program and it failed to ensure the protective measures as specified in CIP-004-1 R3.[8]

[3] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF. When NERC filed VRFs, it originally assigned CIP-004-1 R4.2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-004-1 R4.2 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.
[4] The Mitigation Plan incorrectly stated that it was completed on July 15, 2010.
[5] CIP-005-1 was enforceable from July 1, 2008 (for certain Responsible Entities) through March 31, 2010. CIP-005-2 was enforceable from April 1, 2010 through October 1, 2010 when CIP-005-3 became effective.
[6] CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a "Medium" VRF; R1.6 has a "Lower" VRF.
[7] CIP-006-1 was enforceable from July 1, 2008 (for certain Responsible Entities) through March 31, 2010. CIP-006-2 was enforceable from April 1, 2010 through October 1, 2010 when CIP-006-3 became effective.
[8] Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

CIP-006-2 R1 - OVERVIEW

As a result of a Self-Report, WECC determined that URE did not provide continuous escorted access on June 4, 2010 to individuals without authorized unescorted physical access to URE's Physical Security Perimeters (PSP) and failed to implement and maintain a physical security plan that addressed processes, tools and procedures to monitor physical access to the perimeter(s).

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[9]

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 Orders,[10] the NERC BOTCC reviewed the NOCV and supporting documentation on May 9, 2011. The NERC BOTCC approved the NOCV and the assessment of a twelve thousand two hundred dollar ($12,200) 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 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;

---

assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

[9] *See* 18 C.F.R § 39.7(d)(4).

[10] *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).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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 assessed penalty of twelve thousand two hundred dollars ($12,200) 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 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.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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) Record Disposition Document for Common Information, included as Attachment a;
   i. Disposition Document for CIP-004-1 R4, included as Attachment a-1;
   ii. Disposition Document for CIP-005-1 R1.5, included as Attachment a-2;
   iii. Disposition Document for CIP-006-2 R1, included as Attachment a-3.

b) Record Documents for CIP-004-1 R4:[11]
   i. URE's Self-Report, included as Attachment b-1;
   ii. URE's Mitigation Plan MIT-09-2973, included as Attachment b-2;
   iii. URE's Certification of Mitigation Plan Completion, included as Attachment b-3; and[12]
   iv. WECC's Verification of Mitigation Plan Completion, included as Attachment b-4.

c) Record Documents for CIP-005-1 R1.5:[13]
   i. URE's Self-Report, included as Attachment c-1;
   ii. URE's Mitigation Plan MIT-09-3031, 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-006-2 R1:
   i. URE's Self-Report dated June 25, 2010, included as Attachment d-1;
   ii. URE's Mitigation Plan MIT-10-2972, 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.

A Form of Notice Suitable for Publication[14]
A copy of a notice suitable for publication is included in Attachment e.

[11] Some of the supporting documents refer to the standard as CIP-004-2.
[12] The Certification of Completion was dated July 21, 2010.
[13] Some of the supporting documents refer to the standard as CIP-005-2.
[14] *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	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters 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
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	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
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	*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.
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	

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
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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment a

Disposition Document for Common Information

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-755**

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 **$12,200** FOR **THREE** 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 considered URE's ICP a mitigating factor in determining the penalty for the violations.

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: **11/11/10** OR N/A ☐

SETTLEMENT REQUEST DATE
DATE: OR N/A ☒

NOTICE OF CONFIRMED VIOLATION ISSUED
DATE: **12/17/10** 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-004-1 R4

DISPOSITION OF VIOLATION
Dated May 9, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002154	**WECC2010-607061**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**4**	**4.1, 4.2**	**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-004-1 provides, in pertinent part:

> **Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009….**

CIP-004-1 R4 provides:

> **R4 Access — The Responsible Entity[3] shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.**
>
> **R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and**

[1] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF. When NERC filed VRFs, it originally assigned CIP-004-1 R4.2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-004-1 R4.2 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

[2] At the time of the violations, no VSLs were in effect for CIP-004-1. 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-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.

update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

(Footnotes added).

VIOLATION DESCRIPTION

URE submitted a Self-Report to WECC concerning non-compliance with CIP-004-1 R4.2. According to URE, its parent company's Corporate Security (Corporate Security) employs a security contractor to provide security guards at its facilities, including URE locations housing Critical Cyber Assets (CCAs). Guards that provide security at locations with CCAs are subject to a personnel risk assessment (PRA), and are required to take Critical Infrastructure Protection (CIP) training. After reviewing the PRA and successfully completing training, security guards are provided authorized unescorted physical access to Physical Security Perimeter (PSP) access points via its parent company's access control badge system.

On May 5, 2010, URE inquired about the status of one of the contractor's guards because he/she had not recently been seen on the premises. At that time, the contractor's supervisor notified Corporate Security that the contractor had transferred the guard in question from URE's transmission control center to another office on September 10, 2009. Under established protocols, the contractor is required to notify Corporate Security when a guard no longer requires access to locations housing URE CCAs, and in this case, the contractor did not provide notice for this guard.

According to the contractor, the guard was transferred under a contingency arrangement permitting the guard to be called back from other locations to serve URE locations during emergencies. The contractor has maintained that it is appropriate to keep clearances to PSP access points on the guard's ID badge/card key in the event the guard is recalled to URE facilities. Based on this view, the contractor believed that no notice to URE was required. URE determined it was more prudent to remove CCA access in such cases until such time as the contractor recalls the guard under that contingency arrangement. Therefore, upon learning of the transfer from the contractor, Corporate Security immediately revoked the guard's physical access on May 5, 2010, via URE's access control badge system.

On September 30, 2010, a WECC subject matter expert (SME) began reviewing URE's Self-Report. To complete the review, WECC's SME contacted URE compliance personnel to confirm that URE failed to revoke access to one security guard hired by a contractor, who had authorized unescorted physical access to CCAs. Based on this review, the WECC SME determined that URE was in violation of the Standard because it failed to revoke access within seven calendar days to one individual who URE determined no longer required authorized unescorted physical access to CCAs. WECC's SME forwarded the findings to the WECC Enforcement Department (WECC Enforcement) for its review. After reviewing the SME's findings, WECC Enforcement concurred and found that URE was in violation of CIP-004-1 R4.

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 URE failed to revoke access to only one individual who had physical access to the CCAs. This individual had completed both a PRA and CIP training, and could potentially be recalled to URE facilities by his or her employer, which was an URE contractor. URE revoked the individual's access on the same day that it learned of the individual's reassignment by the contractor.

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) **7/01/09 (date URE had to comply with the Standard) through 7/12/10 (Mitigation Plan completion)**[4]

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] The Mitigation Plan incorrectly stated that it was completed on July 15, 2010.

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2973**
DATE SUBMITTED TO REGIONAL ENTITY	**7/22/10**
DATE ACCEPTED BY REGIONAL ENTITY	**9/30/10**
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
N/A

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**7/12/10**

DATE OF CERTIFICATION LETTER	**7/22/10**[5]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**7/12/10**

DATE OF VERIFICATION LETTER	**10/6/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**7/12/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

- **URE disabled the ID badge/card key in the access control system for the guard who was transferred, and thereby revoked unescorted physical access to CCAs. This action was completed on May 5, 2010.**

- **URE reviewed with the contractor the requirement that physical access to CCAs must be revoked for personnel that are either terminated or assigned to facilities outside of URE or to URE facilities where CCAs are not present. This action was completed May 5, 2010.**

- **URE initiated a new process requiring the contractor to submit a weekly report of guards assigned to URE CCA areas to Corporate Security. SECS will compare that list to the list of personnel with authorized unescorted physical access to CCAs. If the list of personnel with authorized unescorted physical access to CCAs contains any personnel who are not also on the list from the contractor, the access to CCAs will be immediately revoked from the guard's ID badge/card key. URE and the contractor will then determine whether the guard still requires such**

[5] The Certification of Completion was dated on July 21, 2010.

access. If such access is still required, the access will be reinstated on the guard's ID badge/card key. This action was completed on May 27, 2010.

- **URE and Corporate Security conducted a training session with the contractor management team on the importance of NERC CIP requirements. This action was completed on July 12, 2010.**

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)

- **WECC reviewed documents from Corporate Security, including: (1) evidence that the guards badge was disabled; (2) training documents and roster from training; (3) access lists; and (4) process documents for the weekly reports.**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2973

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 R1.5

DISPOSITION OF VIOLATION
Dated May 9, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002236	**WECC2010-610567**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-005-1[1]	**1**	**1.5**	**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-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 R1 provides, in pertinent part:

> **R1. Electronic Security Perimeter — The Responsible Entity[4] shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).**
>
> **R1.5 Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2**

[1] CIP-005-1 was enforceable from July 1, 2008 (for certain Responsible Entities) through March 31, 2010. CIP-005-2 was enforceable from April 1, 2010 through October 1, 2010 when CIP-005-3 became effective.
[2] CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a "Medium" VRF; R1.6 has a "Lower" VRF.
[3] 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.
[4] 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.

and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
(Footnote added).

VIOLATION DESCRIPTION

URE submitted a Self-Report to WECC concerning non-compliance with CIP-005-1 R1.5 and CIP-006-2 R1/1.6. Later, URE found that its original Self-Report for CIP-005-1 R1.5 was not recognized by WECC due to the configuration of WECC's Self-Report portal. Subsequently, WECC requested that URE resubmit a Self-Report specifically expressly referencing CIP-005-1 R1.5. A few months later, URE submitted a Self-Report to WECC for a violation of CIP-005-1 R1.5 because an URE employee performed an escort function without a valid personnel risk assessment (PRA), in violation of URE's own PRA program and the Standard.

During an investigation into having open doors on several server racks in the rear of URE's data center on June 4, 2010, URE discovered that an employee with authorized unescorted access, for nearly a year, to URE's Critical Cyber Assets (CCAs) did not have a valid PRA because the PRA had been inadvertently processed for another employee with the same name. While the employee had completed URE's CIP training, URE immediately revoked the employee's access until the proper PRA could be performed. URE reported that no adverse findings were revealed after the PRA was completed.

On October 13, 2010, a WECC subject matter expert (SME) reviewed URE's Self-Report and Mitigation Plan, and conducted a phone interview with URE's compliance personnel. During the interview, the URE compliance employee stated that the employee in question worked in URE's IT department. The URE employee with authorized unescorted access escorted two other employees requiring escorted access to the facility into an URE data center, to work on equipment in the server racks. The server racks contain backup servers used to monitor electronic security perimeters, and reside within a designated Physical Security Perimeter (PSP). This PSP does not contain CCAs. The URE employee escorted the two other personnel into the PSP, but did not provide continuous escorted access. Several hours later, URE discovered the doors to several server racks were left unlocked. The incident occurred in a building that did not have any CCAs. This person did not have access to any other Cyber Assets.

Based on the evidence submitted and the interview with URE compliance personnel, the WECC SME determined that URE violated the Standard because an URE employee performed an escort function without a valid PRA in violation of URE's own PRA program, and therefore, failed to ensure the protective measures as specified in the requirements of CIP-004-1 R3.[5] The SME forwarded the findings to

[5] Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical

WECC Enforcement for its review. WECC Enforcement reviewed the Self-Report and the SME's findings, and agreed with the SMEs findings that URE was in violation of CIP-005-1 R1.5.

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 employee who did not have a valid PRA did have current CIP training and a background check conducted at the start of employment. Although failure to ensure that CCAs used in the access control and/or monitoring of the ESPs have the appropriate protective measures could result in cyber attacks against CCAs essential to the operation of the BPS, the PSP had video cameras installed, and the video feed was monitored at URE's central monitoring facility.

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) **7/01/09 (date URE had to comply with the Standard) through 6/30/10 (Mitigation Plan completion)**

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

IS THE VIOLATION STILL OCCURRING YES ☐ NO ☒
IF YES, EXPLAIN

---

access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

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-09-3031**
DATE SUBMITTED TO REGIONAL ENTITY	**10/12/10**
DATE ACCEPTED BY REGIONAL ENTITY	**10/14/10**
DATE APPROVED BY NERC	**11/19/10**
DATE PROVIDED TO FERC	**11/22/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**Submitted as complete**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**6/30/10**

DATE OF CERTIFICATION LETTER	**10/12/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**6/30/10**

DATE OF VERIFICATION LETTER	**10/22/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**6/30/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

- **URE reinforced familiarity of all personnel with authorized unescorted access to Physical Security Perimeters (PSP) with the escorted visitor requirements by providing them with the Escorted Visitor procedures for each location to which they have such access. This action was completed on June 16, 2010.**

- **URE conducted an all-hands training session for affected personnel and their management in the affected departments to raise further awareness for CIP-006 physical security issues and escorted visitor requirements. This action was completed on June 16, 2010.**

- **URE installed signage on all applicable server racks in access control and monitoring PSPs (those server racks involved in this event and all other access control and monitoring -related server racks to indicate that the server racks had restricted access and personnel without authorized**

access must be continuously escorted by an authorized personnel. This action was completed on June 30, 2010.

- **URE provided personnel with new authorization for unescorted access to a specific PSP with the Escorted Visitor procedure for the site(s) at which they receive such access.**

- **URE included employee ID numbers in PRA tracking documentation. This action was completed on June 30, 2010.**

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)

- **Evidence the PRA was done for the employee in scope**

- **Evidence that PRAs are tracked using employee numbers**

- **Example of PRA Tracking Spreadsheet with Employee IDs**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report

MITIGATION PLAN
URE's Mitigation Plan MIT-09-3031

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-006-2 R1

DISPOSITION OF VIOLATION
Dated May 9, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
WECC201002152	**WECC2010-610386**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-006-2[1]	**1**	**1.3 and 1.6**	**Medium**	**High[2]**

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

The purpose statement of CIP-006-2 provides: "Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2."

CIP-006-2 R1 provides:

R1. Physical Security Plan — The Responsible Entity[3] shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1 All Cyber Assets within an Electronic Security Perimeter shall 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 such Cyber Assets.

[1] CIP-006-1 was enforceable from July 1, 2008 (for certain Responsible Entities) through March 31, 2010. CIP-006-2 was enforceable from April 1, 2010 through October 1, 2010 when CIP-006-3 became effective.
[2] On December 18, 2009, NERC submitted revised Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for CIP-002-2 through CIP-009-2. On June 20, 2011, FERC issued an order approving the Version 2 VRFs and VSLs and made them effective on April 1, 2010, the date the Version 2 CIP Reliability Standards became effective.
[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 Identification of all physical 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 Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5 Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

R1.6 Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

R1.7 Update of the physical security plan within thirty calendar days of the completion 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 Annual review of the physical security plan.

VIOLATION DESCRIPTION

URE submitted a Self-Report to WECC concerning a violation of CIP-006-2 R1. The violation stems from an event on June 4, 2010, where an employee in URE's Information Security department discovered and reported open doors on the rear of several server racks at an URE data center. The server racks contain backup servers used to monitor Electronic Security Perimeters (ESP), and reside within a designated Physical Security Perimeter (PSP). URE reported that this PSP did not contain Critical Cyber Assets (CCAs).

URE reported that it reviewed the physical access logs for the PSP and discovered that two employees who were not authorized for unescorted access to the PSP were not continuously escorted while working on equipment in the PSP. Access to this PSP is controlled by electronic card key. According to URE, an employee who had authorized unescorted access to this PSP opened the server rack doors for the two employees who did not have authorized unescorted access and left the area while the two employees worked on equipment in the server racks for approximately three hours. When the troubleshooting activities were completed, the two employees

closed and locked the front doors to the server racks, but the rear doors were inadvertently left open. URE physically and electronically examined the Cyber Assets contained within the PSP and found no evidence of tampering. In fact, no physical access to the Cyber Assets took place during the time when the rear cabinet doors were open.

According to URE, the personnel who were not continuously escorted while working on equipment within the PSP are network and server analysts in URE's IT department. Both employees had completed the company's NERC CIP training. In addition, one of the employees had a completed PRA, as prescribed by CIP-004-2 R3, prior to the above occurrence, but did not have authorized unescorted access to the server racks noted above. URE received the PRA documentation for the other employee two days after the occurrence.

On September 30, 2010, a WECC subject matter expert (SME) reviewed the Self-Report and contacted URE compliance personnel. According to URE, there were multiple issues discovered in the scope of their internal audit of the incident. First, URE's security department noticed that doors to several racks were left open at URE's data center. Each of these racks contained three to four servers that were used to monitor traffic within the ESP in scope. Second, when URE reviewed the physical access logs and video feed, it was discovered that two employees who did not have unescorted physical access authorization worked on these server racks, but were not continuously escorted. After the work was done, these employees closed and locked the front door of the cabinet, but the rear door was left open. For these reasons, the SME determined that URE was in violation of CIP 006-2 R1 due to URE's failure to implement a physical security plan that addressed processes, tools and procedures to monitor physical access to the perimeters, and URE's failure to provide continuous escorted access of personnel not authorized for unescorted access with the PSP.

WECC's SME forwarded the findings to WECC's Enforcement Department. WECC Enforcement reviewed the Self-Report and the SME's findings, and agreed that URE was in violation of CIP-006-2 R1.3 due to failure to implement and maintain a physical security plan that addressed processes, tools and procedures to monitor physical access to the perimeter(s) and CIP-006-2 R1.6 due to failure to provide continuous escorted access of personnel not authorized for unescorted access with the PSP.

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 two employees not continuously escorted were URE employees who had undergone CIP training. In addition, one of the employees had a PRA conducted prior to this incident, and the other PRA was completed soon thereafter. Although failure to ensure continuous unescorted access within the PSP for personnel not

authorized for such access could result in malicious harm to CCAs, URE states that the PSP in scope did not contain any CCAs and was under video surveillance at URE's central monitoring facility.

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) **7/01/09 (date URE had to comply with the Standard) through 8/17/10 (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-10-2972**
DATE SUBMITTED TO REGIONAL ENTITY	**7/2/10**
DATE ACCEPTED BY REGIONAL ENTITY	**9/30/10**
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
N/A

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**8/31/10**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**8/17/10**

DATE OF CERTIFICATION LETTER	**8/27/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**8/17/10**
DATE OF VERIFICATION LETTER	**10/6/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**8/17/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

- **URE reinforced familiarity of all personnel with authorized unescorted access to Physical Security Perimeters (PSP) with the escorted visitor requirements by providing them with the Escorted Visitor procedures for each location to which they have such access. This action was completed on June 16, 2010.**

- **URE conducted an all-hands training session for affected personnel and their management in the affected departments to raise further awareness for CIP-006 physical security issues and escorted visitor requirements. This action was completed on June 16, 2010.**

- **URE installed signage on all applicable server racks in access control and monitoring PSPs (those server racks involved in this event and all other access control and monitoring -related server racks) to indicate that the server racks had restricted access and personnel without authorized access must be continuously escorted by an authorized personnel. This action was completed on June 30, 2010.**

- **URE provided personnel with new authorization for unescorted access to a specific PSP with the Escorted Visitor procedure for the site(s) at which they receive such access.**

- **URE included employee ID numbers in PRA tracking documentation. This action was completed on June 30, 2010.**

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)

WECC reviewed documents regarding the following: (1) URE's reinforcement of the escorted visitor requirements; (2) escorted access training materials; (3) an example e-mail of the procedure to follow when escorting visitors; (4) document showing the installation of the signage; (5) procedure to follow if there is an alarm on the server rack; (6) an example of a PRA request; and (7) the PRA tracking spreadsheet.

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2972

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

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