PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

August 31, 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 attached thereto, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This NOP is being filed with the Commission because Texas Reliability Entity, Inc. (Texas RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from Texas RE's determination and findings of the violations of CIP-002-1 Requirement R3, CIP-004-1 R2.2.4, CIP-007-1 R1, CIP-004-1 R3 and R4. According to the Settlement Agreement, URE neither admits nor denies the violations and has agreed to the assessed penalty of eleven thousand dollars ($11,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers TREXXXXXX320, TREXXXXXX321, TREXXXXXX067, TREXXXXXX079 and TREXXXXXX080 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

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

[2] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

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

Statement of Findings Underlying the Violations

This NOP incorporates the findings and justifications set forth in the Settlement Agreement executed on May 20, 2011, by and between Texas RE 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-893	TREXXXXXX320	CIP-002-1	3	High		11,000
	TREXXXXXX321	CIP-004-1	2.2.4	Lower		
	TREXXXXXX067	CIP-007-1	1	Medium		
	TREXXXXXX079	CIP-004-1	3	Medium		
	TREXXXXXX080	CIP-004-1	4	Lower		

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

These violations apply to URE's status as a Responsible Entity.[3]

CIP-002-1 R3 – OVERVIEW

Texas RE conducted a CIP Spot Check of URE at its Control Center.[4] Texas RE determined that URE did not have a complete Critical Cyber Asset (CCA) list. URE's CCA list only contained software applications and did not contain the hardware and data associated with cyber operations of the URE identified Critical Assets.[5]

CIP-004-1 R2/2.2.4 - OVERVIEW

Texas RE conducted a CIP Spot Check of URE at its Control Center. Texas RE determined that URE did not provide training on the plans and procedures to recover or re-establish CCAs and access to these CCAs following a Cyber Security Incident, as required by the Reliability Standard. URE did list the processes and procedures within the training, but did not provide for the training itself.

[3] Within the text of Reliability Standard CIP-002, CIP-004, and 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.

[4] Page 2 of the Settlement Agreement incorrectly lists the Discovery Method as "Audit;" the Disposition Documents correctly list the Discovery Method as "Spot Check."

[5] Cyber Assets are defined as "Programmable electronic devices and communication networks including hardware, software, and data." *Glossary of Terms Used in NERC Reliability Standards*, at pg. 11 (updated May 24, 2011).

CIP-007-1 R1 - OVERVIEW
URE submitted a Self-Report to Texas RE. Texas RE determined that URE did not complete all testing activities before a security update was deployed on six[6] production servers classified as systems supporting CCAs.

CIP-004-1 R3 - OVERVIEW
URE submitted a Self-Report to Texas RE. Texas RE determined that URE did not update a personnel risk assessment for one contract worker. The contract worker did not have an updated criminal check after seven years of working with URE.

CIP-004-1 R4 - OVERVIEW
URE submitted a Self-Report to Texas RE. Texas RE determined that URE did not update its Critical Cyber Asset access list after one employee changed job positions within URE.

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 August 2, 2011. The NERC BOTCC approved the Settlement Agreement, including Texas RE's assessment of an eleven thousand dollar ($11,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. the violations constituted URE's first occurrence of violation of the subject NERC Reliability Standards;
2. URE self-reported the violations of CIP-007-1 R1, CIP-004-1 R3 and R4;
3. Texas RE reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program which Texas RE considered a mitigating factor, as discussed in the Disposition Documents;

[6] Although URE self-reported that the security update was deployed on eight servers, URE later corrected this and confirmed that it was deployed on only six servers.
[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).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. Texas RE 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. Texas RE 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 eleven thousand dollars ($11,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

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

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

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

Attachments to be included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between Texas RE and URE executed May 20, 2011, included as Attachment a;
    i. Disposition of Violation, Information Common to Instant Violations, included as Exhibit A to the Settlement Agreement;

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

ii. Disposition of Violation for CIP-002-1 R3 and CIP-004-1 R2.2.4, included as Exhibit B to the Settlement Agreement;

iii. Disposition of Violation for CIP-007-1 R1, included as Exhibit C to the Settlement Agreement;

iv. Disposition of Violation for CIP-004-1 R3 and R4, included as Exhibit D to the Settlement Agreement;

b) Texas RE's Spot Check Report for CIP-002-1 R3 and CIP-004-1 R2.2.4, included as Attachment b;

c) URE's Self-Report for CIP-007-1 R1, included as Attachment c;

d) URE's Self-Report for CIP-004-1 R3, included as Attachment d;

e) URE's Self-Report for CIP-004-1 R4, included as Attachment e;

f) URE's Revised Mitigation Plan MIT-XX-3079 for CIP-002-1 R3, included as Attachment f;

g) URE's Mitigation Plan MIT-XX-3080 for CIP-004-1 R2.2.4, included as Attachment g;

h) URE's Mitigation Plan MIT-XX-3035 submitted as complete for CIP-007-1 R1, included as Attachment h;

i) URE's Mitigation Plan MIT-XX-1983 for CIP-004-1 R3.3included as Attachment i;

j) URE's Mitigation Plan MIT-XX-1984 for CIP-004-1 R4, included as Attachment j;

k) URE's Certification of Mitigation Plan Completion for CIP-002-1 R3, included as Attachment k;

l) URE's Certification of Mitigation Plan Completion for CIP-004-1 R2.2.4, included as Attachment l;

m) URE's Certification of Mitigation Plan Completion for CIP-004-1 R3 and R4, included as Attachment m;

n) Texas RE's Verification of Mitigation Plan Completion for CIP-002-1 R3, included as Attachment n;

o) Texas RE's Verification of Mitigation Plan Completion for CIP-004-1 R2.2.4, included as Attachment o;

p) Texas RE's Verification of Mitigation Plan Completion for CIP-007-1 R1, included as Attachment p; and

a) Texas RE's Verification of Mitigation Plan Completion for CIP-004-1 R3 and R4, included as Attachment q.

A Form of Notice Suitable for Publication[9]

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

[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	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 Susan D. Vincent* General Counsel Texas Reliability Entity, Inc. 805 Las Cimas Parkway, Suite 200 Austin, TX 78746 (512) 583-4922 susan.vincent@texasre.org Rashida Caraway* Manager, Compliance Enforcement Texas Reliability Entity, Inc. 805 Las Cimas Parkway, Suite 200 Austin, TX 78746 (512) 583-4977 rashida.caraway@texasre.org *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
Texas Reliability Entity, Inc.

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition of Violation, Information Common to Instant Violations

Exhibit "A"

DISPOSITION OF VIOLATION[1]
INFORMATION COMMON TO INSTANT VIOLATIONS
Dated May 10, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	893

REGIONAL ENTITY
Texas Reliability Entity, Inc. (Texas RE)

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 **$11,000** FOR FIVE (5) VIOLATIONS INCLUDED IN THE NOCV/SA VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST ANY CONFIRMED OR SETTLED 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.

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

LIST ANY PRIOR CONFIRMED OR SETTLED 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 ☐
EXPLAIN

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.

URE had a compliance program which Texas RE considered a mitigating factor.

(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: **1/31/2011** OR N/A ☐

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **11/22/2010** 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 ☐ NO CONTEST ☒

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition of Violation for CIP-002-1 R3 and CIP-004-1 R2.2.4

Exhibit "B"

DISPOSITION OF VIOLATION
Dated May 10, 2011

NERC TRACKING NO. **REGIONAL ENTITY TRACKING NO.**
TREXXXXX320
TREXXXXX321

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-002-1	**R3**		**High**	**High**
CIP-004-1	**R2**	**2.2.4**	**Lower**	**Moderate**

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

NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

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. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

CIP-002-1, R3 provides:

Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

VIOLATION DESCRIPTION

During a NERC and Texas RE CIP Spot Check of URE, it was discovered that URE's Critical Cyber Asset (CCA) list was not compliant. URE's CCA list contained only software applications. Based on the NERC Standards Glossary of Terms, as used in CIP-002, the audit team determined that URE's CCA list should contain the hardware and data associated with cyber operations of the URE identified Critical Assets.

CIP-004-1, R2 provides in pertinent part:

Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

VIOLATION DESCRIPTION

URE'S training only "identifies" plans and procedures (business continuity; recovery plan documentation for CCA, performance of regular testing of the recovery plan; and data backup and recovery operating procedure). However, R2.2.4 of CIP-004 states "action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident." This requires the training to include plans and

procedures to recover or re-establish Critical Cyber Assets and access to these Assets following a Cyber Security Incident. However, the listing of these processes and procedures within the training does not equate to provision of training itself as required.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

CIP-002, R3

This violation did not pose a serious or substantial risk to the bulk power system because URE had already applied CIP-003 through CIP-009 on the identified and inventoried hardware associated with cyber operations even though the Critical Cyber Asset list was not updated to include hardware.

CIP-004, R2

This violation did not pose a serious or substantial impact to the bulk power system, because an action plan and procedure to recover or reestablish Critical Cyber Assets did exist. The training for all personnel did identify the names and locations of the procedures that would be used. Although the action plan and procedure may not have been available to all personnel having access to CCAs, the department providing production support of the systems maintains these procedures and its employees have access to these procedures and receives extensive review and training on the procedures. This department is responsible for recovering or re-establishing CCAs.

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) CIP-002, R3
CIP-004, R2

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY Spot Check

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

A. CIP-002-1 (R3) (NERC TRACKING No. TREXXXXX320)

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	MIT-XX-3079
DATE SUBMITTED TO REGIONAL ENTITY	
DATE ACCEPTED BY REGIONAL ENTITY	
DATE APPROVED BY NERC	
DATE PROVIDED TO FERC	

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

The original Mitigation Plan was revised at the request of Texas RE because action items listed in URE's original Mitigation Plan Submittal for CIP-002-1 (listed in Part E.3 of the submitted Mitigation Plan) that were necessary to bring URE in compliance with CIP-002-1, R3 needed to be included in Sections D1 and D3. Section D2 was also updated to reflect any changes to the completion of the Mitigation Plan.

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	Submitted as complete
EXTENSIONS GRANTED	
ACTUAL COMPLETION DATE	

DATE OF CERTIFICATION LETTER
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF

DATE OF VERIFICATION LETTER
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE renamed the inventory lists to the "CCA List" in order to include the hardware associated with Critical Cyber Assets; updated the procedures used to identify Critical Cyber Assets; performed a review of the new procedures to help ensure that they captured the information intended to be included in the CCA List; performed a CIP-003-1 through CIP-009-1 controls assessment, as applicable; and provided training for the new procedures.

Additional milestone activity for above and beyond actions to prevent or minimize the probability of incurring further violations of the same or similar standard included providing classification training as necessary; reviewing CCA change control and configuration management documents; reviewing classification of CCA information and access control to CCA information; reviewing CCA access; providing access controls training as necessary; validating access points and

monitoring systems for the CCA Electronic Security Perimeter and updating documentation as necessary; validating Electronic Security Perimeter access controls including access permissions, ports and services, authentication methods, and monitoring and updating documentation as necessary; updating recovery plan, backup, and restore procedures as needed; updating and executing procedures as needed for security controls testing, security patch management, ports and services management, anti-virus management, account management, security monitoring, disposal or redeployment processes; and identifying and reviewing possible technical exceptions as feasible.

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 submitted to Texas RE a copy of their CCA inventory lists that included the hardware associated with their identified CCAs. Texas RE also reviewed the URE procedures used to identify CCAs. URE also performed a CIP-003 through CIP-009 controls assessment that provided a summary of the tasks within the assessments. All applicable actions in the mitigation plan were completed.

B. CIP-004-1 R2.2.4 (NERC Tracking No. TREXXXXX320)

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. MIT-XX-3080
DATE SUBMITTED TO REGIONAL ENTITY
DATE ACCEPTED BY REGIONAL ENTITY
DATE APPROVED BY NERC
DATE PROVIDED TO FERC

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

MITIGATION PLAN COMPLETED YES ☐ NO ☒

Expected Completion Date Submitted as Complete
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE

DATE OF CERTIFICATION LETTER
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF

DATE OF VERIFICATION LETTER
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE created and published an online training course; identified personnel required to complete the training; notified personnel and department managers of the training requirement; and verified completion of training.

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 submitted to Texas RE a screenshot showing that it published an online training course for recovery training. Texas RE also reviewed printouts of e-mails that identified personnel required to complete the training as well as e-mails that notified managers and personnel of the training requirement. Texas RE reviewed a report of the employees that have taken the recovery training course along with the dates of the training.

EXHIBITS:

URE's Spot Check Report
URE's Mitigation Plan (TREXXXXX320)
URE's Certification of Completion (TREXXXXX320)
Texas RE's Verification of Mitigation Plan Completion (TREXXXXX320)

URE's Mitigation Plan (TREXXXXX321)
URE's Certification of Completion (TREXXXXX321)
Texas RE's Verification of Mitigation Plan Completion (TREXXXXX321)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition of Violation for CIP-007-1 R1

Exhibit "C"

DISPOSITION OF VIOLATION
Dated May 10, 2011

NERC TRACKING NO. **REGIONAL ENTITY TRACKING NO.**
TREXXXXX067

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	**R1**		**Medium**	**Severe**

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

The purpose of Reliability Standard CIP-007, R1 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. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

CIP-007, R1 provides:

Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

VIOLATION DESCRIPTION

During the review of the information provided by URE in the Self-Report, it was determined that, URE's Information Technology initiated plans to accelerate the implementation of a Microsoft security update across the URE environment based upon a Recommendation to Industry issued by NERC. During this accelerated

implementation, the security update was deployed on six production servers classified as system supporting Critical Cyber Assets before all testing activities had been completed.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

This violation did not pose a serious or substantial impact to the bulk power system, because testing activities were completed on the security update. URE implemented the noted security update on the test environment at least two days prior to release to the production systems for verification testing. URE performed security controls testing and there were no issues observed during the testing time. The security update did not adversely impact security controls on the servers.

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)

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-XX-3035
DATE SUBMITTED TO REGIONAL ENTITY	
DATE ACCEPTED BY REGIONAL ENTITY	
DATE APPROVED BY NERC	
DATE PROVIDED TO FERC	

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE Submitted as Complete
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE

DATE OF CERTIFICATION
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF

DATE OF VERIFICATION LETTER
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

To prevent a recurrence, responsibility for patch management of these systems has been transitioned all patching to the department supporting production operations of these systems. Validation testing was performed before the deployment of the patch. Further security controls testing was also performed for the patch after deployment.

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)

Texas RE review of the entity's organizational structure that shows the responsibility of the patch management was transitioned to another department within URE.

EXHIBITS:

URE's Self-Report

URE's Mitigation Plan and Certification of Mitigation Plan Completion

Texas RE's Verification of Mitigation Plan Completion

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition of Violation for CIP-004-1 R3 and R4

Exhibit "D"

DISPOSITION OF VIOLATION
Dated May 10, 2011

NERC TRACKING NO. **REGIONAL ENTITY TRACKING NO.**
TREXXXXXX079
TREXXXXXX080

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**R3**	**3.2**	**Medium**	**Moderate**
CIP-004-1	**R4**	**4.1**	**Lower**	**High**

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

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. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

CIP-004-1, R3 provides:

Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. 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.

CIP-004-1, R4 provides:

Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

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

VIOLATION DESCRIPTION FOR CIP-004-1, R3

Self-Report Finding: URE did not update a personnel risk assessment for a contract worker. One contract worker did not have a criminal check renewal when seven years of service with URE was reached. A review of the records for all contract workers with Critical Cyber Assets access showed that all other criminal history reports were current.

VIOLATION DESCRIPTION FOR CIP-004-1, R4

Self-Report Finding: During a quarterly access review, it was noted that one current employee had two accounts on a Critical Cyber Asset. The employee changed job positions within URE and one of the accounts was requested to be removed. The employee's prior and new position required the same Critical Cyber Asset access. However, the list was not updated within seven days of the request.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

CIP-004-1, R3
This violation did not pose a serious or substantial impact to the bulk power system because an assessment was done on the contractor and all the URE background investigation requirements were met. A review of the records for all contract workers with Critical Cyber Assets access showed that all other criminal history reports were current.

CIP-004-1, R4
This violation did not pose a serious or substantial impact to the bulk power system because the job change still required the employee to have access to the Critical Cyber Asset. The employee had a current personnel risk assessment and training which are mandatory to be authorized for access to Critical Cyber Assets.

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) R3
R4

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 RELATED TO CIP-004-1, R3:

MITIGATION PLAN NO. MIT-XX-1983
DATE SUBMITTED TO REGIONAL ENTITY
DATE ACCEPTED BY REGIONAL ENTITY
DATE APPROVED BY NERC
DATE PROVIDED TO FERC

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE

DATE OF CERTIFICATION LETTER
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF

DATE OF VERIFICATION LETTER
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

1) URE identified all contract workers who have had Critical Cyber Asset access. Records have been reviewed for these contract workers to ensure that a current criminal history has been obtained by the contract worker's employer. Current reports have been confirmed for all other contract workers with Critical Cyber Asset access.
2) URE identified all contract workers who have had Critical Cyber Asset access. Records have been reviewed to ensure that identity verification information is on file. Identity verification has been confirmed for all other contract workers with Critical Cyber Asset access.
3) URE implemented process improvements for annual review of contract worker records to identify any contract worker who must complete an updated criminal history report during the upcoming year. Both the contract worker and their employer will be notified of the requirement of an updated report. URE will suspend logical and physical access for the contractor worker where an updated report is not provided in accordance with identified deadlines.
4) URE implemented revisions to its background check instructions to vendors to require that vendors perform and document identity verification for each contract worker in addition to the previously required criminal history report.
5) URE implemented process improvements to require that vendors provide confirmation of identity verification for any individual who will need unescorted access to URE Critical Cyber Assets. Access is not provided until all documentation is obtained.

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)

Texas RE reviewed a procedure developed to annually review the records of contract workers to identify any contract worker who must complete an updated criminal history report during the upcoming year. Texas RE also reviewed processes that URE implemented, that require vendors to provide confirmation of identity verification for any individual who will need unescorted access to Critical Cyber Assets. Texas RE reviewed a sample of a confirmation sent to URE.

FOR FINAL ACCEPTED MITIGATION PLAN RELATED TO CIP-004-1, R4:

MITIGATION PLAN NO. MIT-XX-1984
DATE SUBMITTED TO REGIONAL ENTITY
DATE ACCEPTED BY REGIONAL ENTITY
DATE APPROVED BY NERC
DATE PROVIDED TO FERC

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE Submitted as Complete
EXTENSIONS GRANTED
ACTUAL COMPLETION DATE

DATE OF CERTIFICATION LETTER
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF

DATE OF VERIFICATION LETTER
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

1) URE has implemented a weekly compliance monitoring process to review contract worker job responsibility changes for those with access to Critical Cyber Assets. The purpose of this process is to monitor management of access permissions related to contract worker's change in responsibilities while at URE. The process is to ensure that access permissions are removed in the event of a change in responsibilities. Contract workers with Critical Cyber Asset access are identified each week. The responsible manager is required to identify if job responsibilities have changed for the noted contract worker(s) and required to review and revise access permissions.
2) This requirement was reiterated with the person responsible for coordinating the removal of this access. Additional awareness information was provided to all URE staff detailing this requirement and their obligation to remove access within seven calendars days of the request. Additionally URE has implemented a process to open Help Desk tickets to be assigned to the appropriate group to have access revoked per the owner's instructions. This ensures that tasks are assigned to a group and not an individual. All open help desk tickets are reviewed daily and the manager of the group is ultimately responsible to ensure completion of the task.
3) Immediately upon discovery, network permissions were restored for the URE staff. The application used to manage permissions was updated to provide better logging and display of response. Additionally, the reviewer of network permissions was made aware of the requirement for the URE staff to have access to all required resources.
4) URE staff has implemented process improvements that require staff members responsible for access review and revocation to applications to provide email responses for each termination notification regardless of applicability of Critical Cyber Asset access. URE staff has implemented process changes for weekly compliance review to ensure the receipt of e-mail confirmation from URE staff as well as reviewing user listings from applicable applications to ensure appropriate revocation of access. Where these actions have not been completed appropriately, URE staff escalates findings to management

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)

Texas RE reviewed a procedure developed to review accesses every fourth quarter for the next year. Texas RE also reviewed processes URE has in place to assign access revocation tickets to appropriate groups and not an individual. A sample list that shows contract workers with Critical Cyber Asset access was reviewed by Texas RE. The list that is sent out weekly for the responsible managers to identify if job responsibilities have changed was reviewed by Texas RE.

EXHIBITS:

URE's Self-Report (TREXXXXXX079)
URE's Self-Report (TREXXXXXX080)

URE's Mitigation Plan (TREXXXXXX079)
URE's Mitigation Plan (TREXXXXXX080)

URE's Certification of Mitigation Plan Completion (TREXXXXXX079 and TREXXXXXX080)
Texas RE's Verification of Mitigation Plan Completion (TRE200900079 and TREXXXXXX080)