NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

February 23, 2011

Ms. Kimberly 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 violation[1] discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Documents (Attachment b), in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This NOP is being filed with the Commission because Reliability*First* Corporation (Reliability*First*) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from Reliability*First*'s determination and findings of the enforceable violations of CIP-007-1 Requirement (R) 4/4.2, CIP-004-1 R4.1 and CIP-007-1 R1.1. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of fifteen thousand dollars ($15,000), in addition to other remedies and actions

[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 (2010). *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).

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 RFC200900166, RFC201000242 and RFC201000243 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This NOP incorporates the findings and justifications set forth in the Settlement Agreement executed on August 30, 2010, by and between Reliability*First* 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-668	RFC200900166	CIP-007-1	4/4.2	Medium[3]	7/1/09-8/14/09	15,000
	RFC201000242	CIP-004-1	4.1	Lower	10/1/09-4/22/10[4]	
	RFC201000243	CIP-007-1	1.1	Medium[5]	12/10/09-4/26/10	

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

CIP-007-1 R4/4.2 - OVERVIEW

On July 20, 2009, URE self-reported a violation of CIP-007-1 R4/4.2. Reliability*First* determined that URE did not implement a process for updating its anti-virus and malware prevention "signatures."

CIP-004-1 R4.1 - OVERVIEW

On January 29, 2009, URE self-reported a violation of CIP-004-1 R4.1. Reliability*First* determined that URE did not perform a quarterly review in the fourth quarter of 2009 of its list of individuals with key cards with authorized unescorted physical access to Critical Cyber Assets, nor conduct quarterly reviews of a key manifest in the third and fourth quarters of 2009.

CIP-007-1 R1.1 - OVERVIEW

On February 3, 2010, URE self-reported a violation of CIP-007-1 R1.1. Reliability*First* determined that URE did not create or implement adequate cyber security test procedures to ensure that changes to Cyber Assets do not adversely affect existing cyber security controls.

[3] The Self-Report and Mitigation Plan both incorrectly state that the violation had a Lower Violation Risk Factor.
[4] The Settlement Agreement incorrectly states the violation was mitigated on April 23, 2010; the correct date is April 22, 2010.
[5] *See* n.3 *supra*.

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

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines, the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on November 2, 2010. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of a fifteen thousand dollar ($15,000) 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. two violations constituted URE's first occurrence of violation of the subject NERC Reliability Standards, while CIP-004-1 R4.1 was a repeat occurrence of CIP-004-1 R4;
2. URE self-reported the violations, although the violation of CIP-004-1 R4.1 was discovered in preparation of an upcoming self-certification;
3. Reliability*First* reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violations which Reliability*First* considered a mitigating factor, as discussed in the Disposition Documents;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. Reliability*First* 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;
7. Reliability*First* considered the repeat violation of CIP-004-1 R4.1 to be an aggravating factor given that the Mitigation Plan associated with the prior violation should have addressed the instant violation; and
8. Reliability*First* 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 approves the Settlement Agreement and believes that the assessed penalty of fifteen thousand dollars ($15,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[6] *See* 18 C.F.R. § 39.7(d)(4).

[7] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009).

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 Notice of Penalty include privileged and 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. Specifically, this includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business and confidential information exempt from the mandatory public disclosure requirements of the Freedom of Information Act, 5 U.S.C. 552, and should be withheld from public disclosure.

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

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

Attachments to be included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between Reliability*First* and URE executed August 30, 2010, included as Attachment a;

   i. URE's Self-Report for CIP-007-1 R4/4.2 dated July 20, 2009, included as Attachment A to the Settlement Agreement;

   ii. URE's Self-Report for CIP-004-1 R4.1 dated January 29, 2009, included as Attachment B to the Settlement Agreement;

   iii. URE's Self-Report for CIP-007-1 R1.1 dated February 3, 2010, included as Attachment C to the Settlement Agreement;

   iv. URE's Mitigation Plan for CIP-007-1 R4/4.2 designated as MIT-09-1930 submitted August 7, 2009, included as Attachment D to the Settlement Agreement;

   v. URE's Certification of Mitigation Plan Completion for CIP-007-1 R4/4.2 dated September 21, 2009, included as Attachment E to the Settlement Agreement;

   vi. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 R4/4.2 dated October 29, 2009, included as Attachment F to the Settlement Agreement;

vii. URE's Mitigation Plan for CIP-004-1 R4.1 designated as MIT-09-2427 submitted March 23, 2010, included as Attachment G to the Settlement Agreement;

viii. URE's Certification of Mitigation Plan Completion for CIP-004-1 R4.1 dated August 25, 2010, included as Attachment H to the Settlement Agreement;[8]

ix. URE's Mitigation Plan for CIP-007-1 R1.1 designated as MIT-09-2428 submitted March 12, 2010, included as Attachment I to the Settlement Agreement;

x. URE's Certification of Mitigation Plan Completion for CIP-007-1 R1.1 dated May 19, 2010, included as Attachment J to the Settlement Agreement;

xi. Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 R1.1 dated June 3, 2010, included as Attachment K to the Settlement Agreement;

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

i. Disposition Document for CIP-007-1 R4/4.2, included as Attachment b-1;

ii. Disposition Document for CIP-004-1 R4.1, included as Attachment b-2;

iii. Disposition Document for CIP-007-1 R1.1, included as Attachment b-3;

c) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R4.1 dated September 3, 2010, included as Attachment c,

A Form of Notice Suitable for Publication[9]

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

[8] Note that the verification for this violation is included in Attachment c to this Notice of Penalty.
[9] *See* 18 C.F.R. § 39.7(d)(6).

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net *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.	Rebecca J. Michael* Assistant General Counsel 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 Robert K. Wargo* Manager of Compliance Enforcement Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 bob.wargo@rfirst.org L. Jason Blake Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 jason.blake@rfirst.org Michael D. Austin* Associate Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 (330) 456-5408 – facsimile mike.austin@rfirst.org

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
Assistant General Counsel
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
ReliabilityFirst Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment b

Disposition Document for Common Information

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS
Dated November 12, 2010

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-668**

REGIONAL ENTITY
ReliabilityFirst Corporation (Reliability*First*)

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 **$15,000** FOR **THREE (3)** VIOLATIONS OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

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

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

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

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ NO ☐ UNDETERMINED ☐
EXPLAIN
URE had a compliance program at the time of the violations which Reliability*First* considered a mitigating factor.

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
The violation of CIP-004-1 R4.1 was a repeat violation.

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

NOTICE OF ALLEGED VIOLATION AND PROPOSED PENALTY OR SANCTION ISSUED
DATE: OR N/A ☒

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **8/13/10** OR N/A ☐

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

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

REGISTERED ENTITY RESPONSE CONTESTED
FINDINGS ☐ PENALTY ☐ BOTH ☐ NO CONTEST ☒

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007-1 R4/4.2

DISPOSITION OF VIOLATION
Dated November 2, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC200900166	**RFC200900166**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	**4**	**4.2**	**Medium**[1]	**High**[2]

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

The purpose statement of CIP-007-1 provides: "Standard CIP-007 requires Responsible Entities[3] 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) . Standards CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. . . ." (Footnote added.)

CIP-007-1 R4 provides:

> **R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).**
>
> **R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.**

[1] The Self-Report and Mitigation Plan both incorrectly state that the violation had a Lower Violation Risk Factor.
[2] At the time of the violation, VSLs for CIP-002 through CIP-009 were not approved by FERC; they were approved on March 18, 2010.
[3] Within the text of Standard CIP-007, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC and Regional Reliability Organizations.

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

VIOLATION DESCRIPTION

On July 7, 2009, URE discovered and on July 20, 2009, URE self-reported possible non-compliance with CIP-007-1 R4.2 to Reliability*First*. URE stated it was unable to access anti-virus software updates transmitted over the Internet from its anti-virus software vendor. As a result, URE was unable to update its anti-virus "signatures," as required by the Standard. URE represented that its inability to access such updates was due to a firewall modification that occurred on May 27, 2009. The firewall modification that prevented URE from accessing anti-virus software updates was required for URE to implement the firewall rules for enforcing one of its Electronic Security Perimeters (ESPs). While URE did conduct testing to ensure this firewall modification would have no operational impact, URE inadvertently omitted connectivity to the anti-virus vendor's Internet update service during the testing. At the time of the violation, URE did not have monitoring in place to provide notification of unsuccessful anti-virus signature updates, but has since implemented this monitoring capability.

This issue affected 43 servers within URE's ESP. Upon correcting the issue and updating anti-virus signatures as necessary, URE scanned the affected servers and found that no viruses or malicious software were present on those servers. Reliability*First* reviewed URE's procedures requiring the use of anti-virus and malware detection software and periodic updates to that software and found that URE failed to implement its process for updating anti-virus and malware prevention signatures in violation of CIP-007-1 R4.2.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because exploitation of URE's failure to update anti-virus software could only be accomplished by a limited number of URE personnel who URE already entrusted with elevated access to a number of other systems within URE. URE's defense in depth strategy included firewalls that limited connectivity to the electronic security perimeter to only known network traffic. Further, URE did have anti-virus and malware protection on the referenced servers, despite its inability to implement anti-virus software updates for the specified period of time.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S) **7/1/09 (when the Standard became mandatory and enforceable for URE) through 8/14/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **7/20/09**

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

REMEDIAL ACTION DIRECTIVE ISSUED YES ☐ NO ☒
PRE TO POST JUNE 18, 2007 VIOLATION YES ☐ NO ☒

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **MIT-09-1930**
DATE SUBMITTED TO REGIONAL ENTITY **8/7/09**
DATE ACCEPTED BY REGIONAL ENTITY **9/4/09**
DATE APPROVED BY NERC **9/10/09**
DATE PROVIDED TO FERC **9/10/09**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **8/21/09**[4]
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **8/14/09**

[4] The Verification of Completion incorrectly states that the proposed completion date was September 21, 2009.

DATE OF CERTIFICATION LETTER **9/21/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **8/14/09**

DATE OF VERIFICATION LETTER **10/29/09**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **8/14/09**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
To mitigate CIP-007-1 R4.2, URE updated its firewall to allow anti-virus signature updates and ensured that the firewall operated properly. URE also created a procedure to allow for manual updates to anti-virus signatures in the event that a similar situation should arise in the future and trained necessary personnel on this new procedure.

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)

- **Attachment A provided evidence of completion that three firewall rules were updated and completed on July 17, 2009. This documentation showed that the firewall changes were requested on July 14, 2009 and approvals were completed on July 16, 2009. This change corrected the problem of the inability to retrieve the new anti-virus signatures via the Internet.**
- **Attachment B provided evidence of monitoring that the anti-virus signatures are updated daily via a scheduled process which was put into effect on July 17, 2009. In the cases where the scheduled process did not successfully retrieve the anti-virus signatures, this evidence showed that the signatures were retrieved manually.**
- **Attachment C provided evidence that the manual update procedure was published and completed on July 31, 2009.**
- **Attachment D – Training Attendance Sign-In Sheet provided evidence that personnel were trained on the manual update procedure on August 14, 2009. Personnel with primary or backup responsibilities for anti-virus signatures, as well as on-call support personnel, reviewed the procedure and signed acknowledging their attendance and the review of the procedure.**
- **On October 19, 2009, URE submitted additional evidence at the request of Reliability*First*. This provided supplemental evidence in support to Attachment A above that the other two rule changes were also made.**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R4/4.2 dated July 20, 2009[5]

MITIGATION PLAN
URE's Mitigation Plan for CIP-007-1 R4/4.2 designated as MIT-09-1930 submitted August 7, 2009[6]

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-007-1 R4/4.2 dated September 21, 2009

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 R4/4.2 dated October 29, 2009

[5] *See* n.1 *supra*.
[6] *Id*.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-1 R4.1

DISPOSITION OF VIOLATION
Dated November 2, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000242	**RFC201000242**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	**4**	**4.1**	**Lower**	**Moderate**

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

The purpose statement of CIP-004-1 provides: "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[1] 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.**

(Footnote added.)

VIOLATION DESCRIPTION

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

On January 13, 2010, URE discovered and on January 29, 2010, URE self-reported non-compliance with CIP-004-1 R4.1 to Reliability*First*. URE maintains two lists of personnel with authorized unescorted physical access to Critical Cyber Assets, including their specific physical access rights to Critical Cyber Assets. The first list documents individuals with physical keycard access and the second list documents individuals with physical door key access. Through its internal compliance testing process in preparation for self-certification, URE found a list of personnel with keycards granting authorized unescorted physical access to Critical Cyber Assets was not reviewed in the fourth quarter of 2009 as required by the Standard. In addition, URE also found a manifest listing individuals with keys granting authorized unescorted physical access to Critical Cyber Assets was not reviewed in the third or fourth quarters of 2009. Upon reviewing the lists as required, URE identified no requisite changes. A formal physical access review was completed on January 15, 2010 and a quarterly review of the physical door key manifest was completed on January 26, 2010.

URE's internal procedures for assessing compliance for its Self-Certification[2] did not identify any deficiencies concerning security training or personnel risk assessments for individuals with authorized unescorted physical access to Critical Cyber Assets. URE did not note any inconsistencies with the processes used to authorize electronic access to Critical Cyber Assets and unescorted physical access to Critical Cyber Assets. Upon review, Reliability*First* found that URE failed to review its lists of individuals with authorized unescorted physical access to Critical Cyber Assets in violation of CIP-004-1 R4.1.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because URE maintained a continuous review of accesses to Critical Cyber Assets as part of its routine security operations. This continuous review consists of the monitoring of electronic access to all Critical Cyber Assets via URE's security logging appliance. Items reviewed include, but are not limited to, system and shared account usage; monitoring for new assets added to Electronic Security Perimeters; and the monitoring of intrusion detection systems. Furthermore, important physical access points were monitored by security guards or video surveillance or both at all times in which URE did not review the referenced lists.

[2] The Self-Certification was for the 2009 time period.

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) **10/1/09 (when the quarterly review was to be performed) through 4/22/10**[3] **(Mitigation Plan completion)**[4]

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **1/29/10**

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

REMEDIAL ACTION DIRECTIVE ISSUED YES ☐ NO ☒
PRE TO POST JUNE 18, 2007 VIOLATION YES ☐ NO ☒

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **MIT-09-2427**
DATE SUBMITTED TO REGIONAL ENTITY **3/23/10**
DATE ACCEPTED BY REGIONAL ENTITY **3/31/10**
DATE APPROVED BY NERC **4/16/10**
DATE PROVIDED TO FERC **4/16/10**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE
N/A
MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **4/23/10**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **4/22/10**

[3] The Settlement Agreement incorrectly states the violation was mitigated on April 23, 2010; the correct date is April 22, 2010.
[4] The Self-Report incorrectly states the violation begin date was July 1, 2009 and the end date was January 26, 2010.

DATE OF CERTIFICATION LETTER **8/25/10**[5]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **4/22/10**

DATE OF VERIFICATION LETTER **9/3/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **4/22/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
To mitigate CIP-004-1 R4.1, URE completed a quarterly review of the access lists at issue. URE also committed to implement a new tool for tracking tasks, including the quarterly review, associated with CIP-004-1 R4.1. This new tool will ensure that future quarterly reviews are not missed.

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)

- **Attachment A – Fourth Quarter 2009 Review of Keycard Access to Control Rooms provided evidence that keycard physical access to control rooms was reviewed for the fourth quarter of 2009 on January 15, 2010.**
- **Attachment B – Fourth Quarter 2009 Review of Keycard Access to Computer Rooms provided evidence that keycard physical access to computer rooms was reviewed for the fourth quarter of 2009 on January 14, 2010.**
- **Attachment C – Quarter 2010 Review of the Key Manifest provided evidence that the key manifest was reviewed for the first quarter of 2010 on January 25, 2010 and that no access changes were required.**
- **Attachment D provided evidence that URE's compliance tracking tool was implemented and will ensure that future reviews are not missed. Tasks will be sent to Physical Security to perform quarterly physical access reviews for keycards and of the key manifest.**
- **Evidence that outlines the physical security process for access control, quarterly reviews, and recertification for personnel that have physical access to Critical Cyber Assets. The quarterly review section summarizes the quarterly review of users with badge or key access to critical physical areas by members of the Physical Security group and critical area owners. This process is driven from an electronic work flow that is started with a task reminder that generates a report (list) of users with physical access to critical areas. This list is then reviewed by both Physical Security staff and the manager and/or owning area manager and updated as necessary. The procedure also includes an access review checklist that is filled out each time physical access is granted or updated.**

[5] The Certification of Completion letter incorrectly states that the proposed completion date was May 30, 2010.

EXHIBITS:

SOURCE DOCUMENT[6]
URE's Self-Report for CIP-004-1 R4.1 dated January 29, 2010

MITIGATION PLAN
URE's Mitigation Plan for CIP-004-1 R4.1 designated as MIT-09-2427 submitted March 23, 2010

CERTIFICATION BY REGISTERED ENTITY[7]
URE's Certification of Mitigation Plan Completion for CIP-004-1 R4.1 dated August 25, 2010

VERIFICATION BY REGIONAL ENTITY
Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R4.1 dated September 3, 2010

[6] *See* n.5 *supra*.
[7] *See* n.6 *supra.*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007-1 R1.1

DISPOSITION OF VIOLATION
Dated November 12, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
RFC201000243	**RFC201000243**

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	**1**	**1.1**	**Medium**[1]	**High**

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

The purpose statement of CIP-007-1 provides: "Standard CIP-007 requires Responsible Entities[2] to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…." (Footnote added.)

CIP-007-1 R1 provides:

> **R1. 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.**

VIOLATION DESCRIPTION

[1] The Self-Report and Mitigation Plan both incorrectly state that the violation had a Lower Violation Risk Factor.

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

On January 29, 2010, URE discovered and on February 3, 2010, URE self-reported possible non-compliance with CIP-007-1 R1.1 to Reliability*First*. According to the Self-Report, on December 10, 2009, URE installed and configured a SQL Server database on a new Cyber Asset residing in one of URE's Electronic Security Perimeters (ESPs). Upon installing this new database, URE tested the impact on cyber security controls as to both the database itself and the database's underlying operating system. Testing demonstrated that the database's operating system did not adversely affect cyber security controls.

URE later discovered that its test procedures were inadequate for testing the impact of the database itself on cyber security controls. Prior to the installation of the new database, URE's test procedures proved to be adequate. URE's testing procedures required the use of third-party software applications for automated testing of cyber security controls. The new database, however, was not configured to run this third party software, making URE's documented test procedures inadequate for testing this database. As a result, URE developed new manual cyber security control test procedures to test this database.

Upon performing these manual inspections, URE discovered that three of the SQL Server database's cyber security controls did not conform to URE's cyber security controls, as defined in its documentation. URE's use of a database default setting during installation introduced three cyber security controls that did not conform to URE's referenced cyber security controls. The first two non-conforming cyber security controls related to the configuration of how access is authorized. The third non-conforming cyber security control related to the manner in which inter-process communication occurs within the server. Upon review, Reliability*First* found that URE failed to create and implement cyber security test procedures to ensure that changes to Cyber Assets do not adversely affect existing cyber security controls.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

Reliability*First* determined that the violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because during the installation, URE was monitoring the system to confirm that the automatic testing procedure was adequate. Upon discovering that its documented test procedures would not adequately test the new database's impact on cyber security controls, URE developed and implemented manual testing methods beyond the scope of the program. Therefore, there was a minimal period, monitored by URE, where changes to Cyber Assets did not adversely affect existing cyber security controls

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) **12/10/09 (when the procedures became inadequate) through 4/26/10 (Mitigation Plan completion)**[3]

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **2/3/10**

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2428**
DATE SUBMITTED TO REGIONAL ENTITY	**3/12/10**
DATE ACCEPTED BY REGIONAL ENTITY	**3/31/10**
DATE APPROVED BY NERC	**4/16/10**
DATE PROVIDED TO FERC	**4/16/10**

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

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**4/30/10**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**4/26/10**

[3] The Settlement Agreement incorrectly states that the violation began on December 10, 2009, when the new database was installed and configured. The Self-Report incorrectly states that the violation ended on February 3, 2010.

DATE OF CERTIFICATION LETTER **5/19/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **4/26/10**

DATE OF VERIFICATION LETTER **6/3/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **4/26/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE
To mitigate CIP-004-1 R1.1, URE updated its testing on the SQL Server database. URE also committed to update its testing methodology to include procedures to adequately test cyber security controls associated with all URE Critical Cyber Assets and to train all necessary personnel on this updated methodology.

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)

- **Attachment A – Evidence that test procedures were completed against the SQL Server.**
- **Attachment B – Copy of the previous SQL Server Test Procedures was provided to show the version in place at the time of the violation.**
- **Attachment C – Copy of the updated SQL Server Test Procedures provided evidence that the SQL Server Test Procedure was published and completed.**
- **Attachment D – Training Attendance Sign-In Sheet provided evidence that personnel were trained on the SQL Server Test Procedure. All database administrators signed acknowledging their attendance and the review of the procedure.**

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-007-1 R1.1 dated February 3, 2010[4]

MITIGATION PLAN
URE's Mitigation Plan for CIP-007-1 R1.1 designated as MIT-09-2428 submitted March 12, 2010[5]

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-007-1 R1.1 dated May 19, 2010

[4] *See* n.1 *supra*. The Self-Report incorrectly states that the violation ended on February 3, 2010.
[5] *See* n.1 *supra*.

VERIFICATION BY REGIONAL ENTITY

ReliabilityFirst's Verification of Mitigation Plan Completion for CIP-007-1 R1.1 dated June 3, 2010