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 Settlement Agreement (Attachment f) 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 the Florida Reliability Coordinating Council, Inc. (FRCC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from FRCC's determination and findings of the enforceable violations of CIP-004-1 Requirement (R) 2.1, CIP-004-1 R3, CIP-004-2 R3, and two instances of CIP-005-1 R1. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of seventeen thousand dollars ($17,000), 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

[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

NERC Violation Tracking Identification Numbers FRCC200900278, FRCC200900217, FRCC201000383, FRCC201000384[3] and FRCC200900277 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 May 16, 2011, by and between FRCC 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-634	FRCC200900278	CIP-004-1	2.1	Medium[4]	9/7/09 – 12/14/09	17,000
	FRCC200900217	CIP-004-1	3	Medium[5]	6/7/09 – 7/23/09	
	FRCC201000383	CIP-004-2	3	Medium	4/29/10 – 6/8/10	
	FRCC201000384	CIP-005-1	1	Lower	7/1/09 – 3/29/10	
	FRCC200900277	CIP-005-1	1.4	Lower	7/1/09 – 10/27/09	

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 R2.1 - OVERVIEW

As a result of a spot-check, FRCC determined that URE did not provide sufficient training to one of its employees who had access to Critical Cyber Assets.

[3] URE self-reported possible violations for CIP-005-1 R1.4 (FRCC201000368) and CIP-005-1 R1.6 (FRCC201000369) on May 17, 2010. FRCC Compliance Enforcement determined these two sub-requirement possible violations should be rolled-up to one R1 violation (FRCC201000384).

[4] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" Violation Risk Factor (VRF); R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 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 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[5] CIP-004-1 R3 has a "Medium" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 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 R3 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

CIP-004-1 R3 - OVERVIEW
As a result of a Self-Report on July 31, 2009, FRCC determined that URE did not conduct a background check within the thirty-day period provided for in the Standard on a contractor who was allowed access to URE's Physical Security Perimeter (PSP).

CIP-004-2 R3 - OVERVIEW
As a result of a Self-Report on July 16, 2010, FRCC determined that URE did not revoke the access rights of an employee to a PSP after the employee's personnel risk assessment expired.

CIP-005-1 R1 - OVERVIEW
As a result of a Self-Report on May 17, 2010, FRCC determined that URE did not include eight digital wall clocks and a server on its Cyber Asset list.

As a result of a Self-Report on November 5, 2009, FRCC determined that URE did not include thirteen new energy management system personal computers as Non-Critical Cyber Assets on its Critical Cyber Asset listing until October 27, 2009.

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 January 20, 2011. The NERC BOTCC approved the Settlement Agreement, including FRCC's assessment of a seventeen thousand dollar ($17,000) 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:[8]

1. URE self-reported the violations for CIP-004-1 R3, CIP-004-2 R3, and two instances of a violation of CIP-005-1 R1;
2. FRCC reported that URE was cooperative throughout the compliance enforcement process;
3. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

[6] *See* 18 C.F.R. § 39.7(d)(4).
[7] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).
[8] FRCC considered URE's compliance program as a neutral factor in the penalty determination, as discussed in the Disposition Document.

4. FRCC determined that the violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), as discussed in the Disposition Documents; and
5. FRCC 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. The NERC BOTCC believes that the assessed penalty of seventeen-thousand dollars ($17,000) 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 part of this NOP are the following documents:

a) FRCC's Information Sheet for CIP-004-1 R2.1, included as Attachment a;

b) URE's Self-Report for CIP-004-1 R3 dated July 31, 2009, included as Attachment b;

c) URE's Self-Report for CIP-004-2 R3 dated July 16, 2010, included as Attachment c;

d) URE's Self-Report for CIP-005-1 R1 dated May 17, 2010, included as Attachment d;

e) URE's Self-Report for CIP-005 R1.4 dated November 6, 2009, included as Attachment e;

f) Settlement Agreement by and between FRCC and URE executed May 16, 2011, included as Attachment f;

   i. Disposition Document for Common Information, included as Attachment A to the Settlement Agreement;

   ii. Disposition Document for CIP-004-1 R2.1, CIP-004-1 R3 and CIP-004-2 R3 included as Attachment B to the Settlement Agreement;

   iii. Disposition Document for CIP-005-1 R1 and CIP-005-1 R1.4, included as Attachment C to the Settlement Agreement;

g) URE's Mitigation Plan MIT-10-2721 for CIP-004-1 R2.1 submitted December 17, 2009, included as Attachment g;

h) URE's Mitigation Plan MIT-09-2208 for CIP-004-1 R3 submitted July 31, 2009, included as Attachment h;

i) URE's Mitigation Plan MIT-10-3480 for CIP-004-2 R3 submitted July 16, 2010, included as Attachment i;[9]

j) URE's Mitigation Plan MIT-09-2720 for CIP-005-1 R1 submitted May 17, 2010, included as Attachment j;

k) URE's Revised Mitigation Plan MIT-09-2720 for CIP-005-1 R1 submitted August 19, 2010, included as Attachment k;

l) URE's Mitigation Plan MIT-09-3346 for CIP-005-1 R1.4 submitted November 5, 2009, included as Attachment l;

m) URE's Certification of Mitigation Plan Completion for CIP-004-1 R2.1 dated December 17, 2009, included as Attachment m;

n) URE's Certification of Mitigation Plan Completion for CIP-004-1 R3 submitted September 30, 2009,[10] included as Attachment n;

[9] On August 26, 2010, NERC submitted an approved Mitigation Plan designated as MIT-10-2721for NERC Violation Tracking ID# FRCC201000383. NERC subsequently discovered that MIT-10-2721 was incorrectly associated with FRCC201000383. By copy of this notice, NERC hereby notifies FERC that MIT-10-2721 is associated with FRCC201000278.

[10] URE's Certification is undated but was submitted to FRCC on September 30, 2009.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

o) URE's Certification of Mitigation Plan Completion for CIP-005-1 R1 dated February 7, 2011, included as Attachment o;

p) URE's Certification of Mitigation Plan Completion for CIP-005-1 R1.4 dated December 29, 2009, included as Attachment p;

q) FRCC's Verification of Mitigation Plan Completion for CIP-004-1 R2.1 dated February 18, 2011, included as Attachment q;

r) FRCC's Verification of Mitigation Plan Completion for CIP-004-1 R3 dated February 18, 2011, included as Attachment r; and

s) FRCC's Verification of Mitigation Plan Completion for CIP-005-1 R1 and R1.4 dated February 7, 2011, included as Attachment s.

A Form of Notice Suitable for Publication[11]

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

[11] *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 Sarah Rogers* President and Chief Executive officer Florida Reliability Coordinating Council, Inc. 1408 N. Westshore Blvd., Suite 1002 Tampa, Florida 33607-4512 (813) 289-5644 (813) 289-5646 – facsimile srogers@frcc.com Linda Campbell* VP and Executive Director Standards & Compliance Florida Reliability Coordinating Council, Inc. 1408 N. Westshore Blvd., Suite 1002 Tampa, Florida 33607-4512 (813) 289-5644 (813) 289-5646 – facsimile lcampbell@frcc.com Barry Pagel* Director of Compliance Florida Reliability Coordinating Council, Inc. 3000 Bayport Drive, Suite 690 Tampa, Florida 33607-8402 (813) 207-7968 (813) 289-5648 – facsimile bpagel@frcc.com	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça* 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 sonia.mendonca@nerc.net Richard Gilbert* Manager of Compliance Enforcement Florida Reliability Coordinating Council, Inc. 3000 Bayport Drive, Suite 690 Tampa, Florida 33607-8402 (813) 207-7991 (813) 289-5648 – facsimile rgilbert@frcc.com *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
Sonia C. Mendonça
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
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Florida Reliability Coordinating Council, Inc.

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for Common Information

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

DISPOSITION OF VIOLATION[1]

INFORMATION COMMON TO INSTANT VIOLATIONS
Dated May 16, 2011

REGISTERED ENTITY	NERC REGISTRY ID	NOC#
Unidentified Registered Entity (URE)	**NCRXXXXX**	**NOC-634**

REGIONAL ENTITY
Florida Reliability Coordinating Council, Inc. (FRCC)

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 **$17,000** FOR **FIVE** 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
There is a documented internal compliance program (ICP) that has been signed by a senior officer or equivalent. FRCC did not consider URE's ICP as a factor in determining the penalty.

EXPLAIN SENIOR MANAGEMENT'S ROLE AND INVOLVEMENT WITH RESPECT TO THE REGISTERED ENTITY'S COMPLIANCE PROGRAM, INCLUDING WHETHER SENIOR MANAGEMENT TAKES ACTIONS THAT SUPPORT THE COMPLIANCE PROGRAM, SUCH AS TRAINING, COMPLIANCE AS A FACTOR IN EMPLOYEE EVALUATIONS, OR OTHERWISE.

(4) ANY ATTEMPT BY THE REGISTERED ENTITY TO CONCEAL THE VIOLATION(S) OR INFORMATION NEEDED TO REVIEW, EVALUATE OR INVESTIGATE THE VIOLATION.

YES ☐ NO ☒
IF YES, EXPLAIN

(5) ANY EVIDENCE THE VIOLATION(S) WERE INTENTIONAL (IF THE RESPONSE IS "YES," THE ABBREVIATED NOP FORM MAY NOT BE USED.)

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☐
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

OTHER RELEVANT INFORMATION:

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

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **7/22/10 for CIP-004-1 R2.1, CIP-004-1 R3, CIP-004-2 R3 and CIP-005-1 R1.4; and 8/18/10 for CIP-005-1 R1** OR N/A ☐

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

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

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-1 R2.1, CIP-004-1 R3 and CIP-004-2 R3

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

DISPOSITION OF VIOLATION
Dated May 16, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
FRCC200900278	**URE_2009_08**
FRCC200900217	**URE_2009_04**
FRCC201000383	**FRCC2010-100390**

I. VIOLATION INFORMATION[1]

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)[2]
CIP-004-1	**2**	**2.1**	**Lower[3]**	**N/A**
CIP-004-1	**3**		**Lower[4]**	**N/A**
CIP-004-2	**3**		**Medium**	**High**

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

The purpose statement of CIP-004-1, and CIP-004-2 provide 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[]…."

[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.

[2] At the time of the violations, no VSLs were in effect for CIP-004. 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] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" Violation Risk Factor (VRF); R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 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 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[4] CIP-004-1 R3 has a "Medium" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 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 R3 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

CIP-004-1 R2 provides in pertinent part:

R2. Training - The Responsible Entity[5] 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.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

CIP-004-1 R3 provides:

R3. 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.

[5] 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.

CIP-004-2 R3 provides in pertinent part:

> **R3. 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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment 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-004-2.**

VIOLATION(S) DESCRIPTION

<u>CIP-004-1 R2.1</u>: At a spot check, FRCC found that URE did not provide sufficient evidence to demonstrate that one of its employees having authorized cyber access to Critical Assets received training within ninety calendar days of when access was authorized, thereby violating Standard CIP-004-1 R2.1. It was discovered that an employee of URE had been granted cyber access to the Energy Control Center (ECC) and Critical Cyber Assets on June 8, 2009, and that employee took the required training 105 days later on September 21, 2009. The violation duration existed from September 7, 2009 to September 20, 2009.

<u>CIP-004-1 R3</u>: On July 31, 2009, URE submitted a Self-Report to FRCC indicating that two contract employees (a father and son with the same first and last names), were approved for NERC access to the Physical Security Perimeter (PSP), but

background checks had only been performed on one of the contractors (the father). Unescorted physical access for the son was granted without a personnel risk assessment (PRA) having been done on 5/8/2009. The PRA was due within 30 days of access being granted according to the language in CIP-004-1. The discrepancy was identified on 7/16/09 by URE, while manually verifying training conducted on an old training system. At that time, URE's IT security personnel were notified, and they immediately removed the son's access. The PRA was completed on 7/21/09, and access was re-enabled for the son.

CIP-004-2 R3:[6] On July 16, 2010, URE submitted a Self-Report to FRCC indicating that it had discovered that two individuals were given authorized unescorted physical access or authorized cyber access to protected Cyber Assets without valid PRAs. For these individuals, one was provided only unescorted physical access while the other was only provided cyber access to the Cyber Assets.

URE's program for conducting PRAs for granting authorized unescorted physical access or authorized cyber access to Critical Cyber Assets required that a PRA be conducted on or after January 1, 2007, as a prerequisite to personnel being granted authorized cyber access or authorized unescorted physical access to protected Cyber Assets.

The first individual was an employee who was granted authorized unescorted physical access rights to a PSP housing Critical and Non-Critical Cyber Assets on April 29, 2010 through May 6, 2010. The most recent PRA for that employee was conducted on August 30, 1999. This was due to human errors by IT Security Analysts in a twice-monthly manual process for verifying the PRA date for personnel with authorized unescorted physical access or authorized cyber access to protected Cyber Assets. On May 6, 2010, an IT Security Analyst detected the error and immediately revoked access.

The second individual was a contractor who was given authorized cyber access to Non-Critical Cyber Assets used in the monitoring and control of electronic and physical access on June 8, 2010, before his PRA was conducted. This was due to a workflow flaw in the system. A recently implemented automated alerting process notified IT Security personnel later that day. IT Security personnel then reviewed the access and immediately revoked access within hours after it was granted.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

FRCC determined that the violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:

[6] FRCC treated this CIP-004 R3 violation separately from the previous violation because the previous violation had already been mitigated and closed before the second violation was reported to FRCC.

a. **<u>For CIP-004-1 R2.1</u>: The employee in question completed the cyber security training in 2007 (11/5/07) that was required by the company prior to granting cyber or physical access under URE's program for compliance with the Urgent Action 1200 standards. The training focused on such things as employee responsibilities for cyber and physical access such as escorting procedures, *etc*. This program was replaced in 2008 with a more robust training program that addressed all elements of the NERC CIP Version 1 standards that became compliant in July of 2008.**

b. **<u>For CIP-004-1 R3</u>: URE has a PRA program, but one assessment was not conducted as required. Upon discovery of the violation, access was immediately disabled (for the son) until the background check was performed and cleared and access was re-enabled. According to responses to follow-up questions from the FRCC, URE responded that the contractor without the correct background check was trained on URE's cyber security program on 7/14/08, and was only granted physical access to Critical Cyber Assets. When the background check was processed on 7/16/09, a clear report was returned on 7/21/09. In addition, the physical access to the Critical Cyber Assets by the unchecked contract employee only lasted one day, 5/8/09.**

c. **<u>For CIP-004-2 R3</u>: During the period when the employee had unescorted physical access rights, April 29, 2010 through May 6, 2010, she did not exercise unescorted physical access to NERC Cyber Assets. This was confirmed by a review of the cardkey access logs and an attestation from the employee's supervisor. The individual was a long-term employee who had previously successfully completed a personnel risk assessment in 1999. An updated PRA was successfully completed on May 13, 2010 and unescorted physical access was then restored.**

The contractor was granted cyber access on June 8, 2010, but the problem was detected through use of the newly implemented automated daily alerting system at 6:00 p.m. that same day and revoked twelve minutes later. During the period of time that the contractor had cyber access on June 8, 2010, his only actual cyber access was his initial sign on, at 4:38 p.m., to change his temporary password, which was witnessed by a URE employee. Cyber access was restored on June 13, 2010, following the receipt of results of the PRA.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT	☒[7]
SELF-CERTIFICATION	☐
COMPLIANCE AUDIT	☐
COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK	☒[8]
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

DURATION DATE(S)

CIP-004-1 R2.1: 9/7/09 (ninety-day period for conducting training begins) -12/14/09 (Mitigation Plan completion)

CIP-004-1 R3: 6/7/09 (background check on contract employee was required to be performed) -7/23/09 (Mitigation Plan completion)

CIP-004-2 R3: 4/29/10 (employee granted authorized unescorted physical access and authorized cyber access to Cyber Assets without a PRA) through 6/8/10 (date access revoked to cyber security assets to contractor without a PRA)[9]

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY

CIP-004-1 R2.1: Spot Check

CIP-004-1 R3: 7/31/09

CIP-004-2 R3: 7/16/10

IS THE VIOLATION STILL OCCURRING	YES	☒[10]	NO	☒

IF YES, EXPLAIN
The Mitigation Plan for the CIP-004-2 R3 violation is not expected to be completed until June 30, 2011.

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

[7] URE's violations of CIP-004-1 R3 and CIP-004-2 R3 were discovered through Self-Report.
[8] URE's violation of CIP-004-1 R2.1 was discovered via a Spot Check.
[9] Mitigation Plan for CIP-004-2 R3 violation is not expected to be completed until June 30, 2011.
[10] *Id*.

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. **CIP-004-1 R2.1: MIT-10-2721**
CIP-004-1 R3: MIT-09-2208
CIP-004-2 R3: MIT-10-3480[11]

DATE SUBMITTED TO REGIONAL ENTITY **CIP-004-1 R2.1: 12/17/09**
CIP-004-1 R3: 7/31/09
CIP-004-2 R3: 7/16/10

DATE ACCEPTED BY REGIONAL ENTITY **CIP-004-1 R2.1: 7/16/10**
CIP-004-1 R3: 11/16/09
CIP-004-2 R3: 7/22/10

DATE APPROVED BY NERC **CIP-004-1 R2.1: 8/26/10**
CIP-004-1 R3: 12/29/09
CIP-004-2 R3: 4/13/11

DATE PROVIDED TO FERC **CIP-004-1 R2.1: 8/26/10**
CIP-004-1 R3: 12/29/09
CIP-004-2 R3: 4/15/11

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

MITIGATION PLAN COMPLETED YES ☒[12] NO ☒

EXPECTED COMPLETION DATE
CIP-004-1 R2.1: Submitted as complete
CIP-004-1 R3: Submitted as complete
CIP-004-2 R3: 6/30/11

EXTENSIONS GRANTED **N/A**

ACTUAL COMPLETION DATE **CIP-004-1 R2.1: 12/14/09**
CIP-004-1 R3: 7/23/09
CIP-004-2 R3: TBD[13]

[11] On August 26, 2010, NERC submitted an approved Mitigation Plan designated as MIT-10-2721for NERC Violation Tracking ID# FRCC201000383. NERC subsequently discovered that MIT-10-2721 was incorrectly associated with FRCC201000383.
[12] Mitigation Plans for violations of CIP-004-1 R2.1 and CIP-004-1 R3 were submitted as complete, however, the Mitigation Plan for CIP-004-2 R3 has an expected completion date of June 30, 2011.
[13] *See* n.10.

DATE OF CERTIFICATION LETTER **CIP-004-1 R2.1: 12/17/09**
CIP-004-1 R3: 9/30/09[14]
CIP-004-2 R3: TBD

CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF
CIP-004-1 R2.1: 12/14/09
CIP-004-1 R3: 7/23/09
CIP-004-2 R3: TBD

DATE OF VERIFICATION LETTER
`
CIP-004-1 R2.1: 2/18/11[15]
CIP-004-1 R3: 2/18/11[16]
CIP-004-2 R3: TBD

VERIFIED COMPLETE BY REGIONAL ENTITY AS OF
CIP-004-1 R2.1: 12/14/09
CIP-004-1 R3: 7/23/09
CIP-004-2 R3: TBD

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

CIP-004-1 R2.1
URE implemented a new procedure for documenting completion of the NERC CIP Compliance training where specifics of each completion are automatically uploaded into an SAP Human Resources database on a nightly basis. The IT Security analysts validate the completion of training by determining if training was completed according to the entry in the SAP, which cannot be confused with any other training information. Additionally, the extract file that contained the training data for all the completed classes from the prior system was removed and therefore there is no confusion on obtaining the correct date for the NERC completion.

CIP-004-1 R3
Access for the contractor (the son) was immediately disabled on July 16, 2009 when the discrepancy was identified. The background check was submitted for the contractor (the son) on July 17, 2009. The manual paperwork process of updating and submitting a spreadsheet from Purchasing to IT Security

[14] URE's Certification is undated but was submitted to FRCC on September 30, 2009.
[15] The Verification of Completion incorrectly states that the FRCC200900228 violation is CIP-004-1 R2.1 instead of CIP-004-1 R3.
[16] The Verification of Completion incorrectly states that the FRCC200900217 violation is CIP-004-1 R3 instead of CIP-004-1 R2.1.

has been replaced with a data entry directly into SAP by the background check approver.

CIP-004-2 R3

To reduce the likelihood of reoccurrence of these errors, URE has implemented the following mitigating actions:

1. Employee Coaching – A meeting was held between the manager of Information Security and the employee that made the error. This meeting stressed the importance of following all NERC processes and procedures.

2. IT Security Training – A meeting was held with the entire Information Security team to review the process for verifying NERC PRA dates.

3. SAP Human Resources Validation Screens – A new visual compliance indicator was added to the screens within the SAP Human Resources system used by the security analysts to verify PRA dates.

4. E-mail Alerts – An enhanced automated, daily detective control was implemented that checks for non-compliance situations of PRA dates.

5. Training on the new SAP Human Resources screen – The Information Security access administration team, which performs the verifications, was trained on the new visual indicator located in the SAP Human Resources system.

6. Chief Information Officer held all-hands meetings. These meetings with Information Technology personnel stressed the importance of following NERC compliance processes.

To further reduce the likelihood of errors, URE has planned the following mitigating actions:

7. URE is in the process of moving the system to a new platform that will ultimately provide additional workflow capabilities, including integration with URE's SAP Human Resources system. This will enable URE to enhance its access request process to minimize future instances of unauthorized access by preventing personnel from entering requests for access to NERC Cyber Assets prior to the existence of a valid PRA record in the SAP Human Resources system.

The project, which will be completed and implemented by June 30, 2011, consists of the following major milestones:

a) Develop web front end modifications to existing system for employee and contractor requests. This functionality will provide additional assurance on security access requests which will identify requests where a NERC PRA is required.

b) Define requirements for a workflow solution and develop an implementation plan for a new Information Access System.

c) Develop functional and system testing plans for the new workflow changes.

d) Conduct training on new Information Access System

e) Implement final Information Access System modifications for employees and contractors workflow improvements, and tie to the SAP Human Resources system.

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)

CIP-004-1 R2.1

Screenshot of Employee Training Record from the SAP Human Resources Database	**Undated**
A document that lists the training courses of the employee in question, and shows the employee attended the NERC training course on 9/21/09	**Dated 4/29/10**
A procedure document details the process for verifying NERC CIP Compliance needed to allow access to NERC CIP cyber assets.	**Dated 4/29/10**
A calendar entry for a scheduled meeting on access verification procedure changes	**Dated 4/12/10**

CIP-004-1 R3

A document that shows the contractor's access and NERC locations that were accessed by the cardkey	**7/15/09**
A document that shows the cardkey was edited on July 16th at 11:44 AM to disable NERC access	**7/16/09**
An attestation email detailing the removal of NERC card key access for the "contractor"	**9/24/09**
Background Check for the "contractor"- This document shows that a background check was done for the "contractor" on 7/21/09	**7/20/09**
A document that shows the background check information was entered into the SAP Human Resources database	**7/21/09**

A document that shows a new procedure detailing how to enter the background check date into the SAP database in a flowchart for handling NERC access and background checks for contractors	**Undated**
A document that shows the new check and balance procedure was revised on 7/23/09. Items 9 and 10 are specific to contractor entries in the SAP database.	**7/23/09**

CIP-004-2 R3
TBD

EXHIBITS:

SOURCE DOCUMENT
FRCC's Source Document for CIP-004-1 R2.1

URE's Self-Report for CIP-004-1 R3 dated July 31, 2009

URE's Self-Report for CIP-004-2 R3 dated July 16, 2010

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2721 for CIP-004-1 R2.1submitted December 17, 2009

URE's Mitigation Plan MIT-09-2208 for CIP-004-1 R3 submitted July 31, 2009

URE's Mitigation Plan MIT-10-3480 for CIP-004-2 R3 submitted July 16, 2010

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-004-1 R2.1 dated December 17, 2009

URE's Certification of Mitigation Plan Completion for CIP-004-1 R3 submitted September 30, 2009[17]

VERIFICATION BY REGIONAL ENTITY
FRCC's Verification of Mitigation Plan Completion for CIP-004-1 R2.1 dated February 18, 2011

FRCC's Verification of Mitigation Plan Completion for CIP-004-1 R3 dated February 18, 2011

[17] URE's Certification is undated but was submitted to FRCC on September 30, 2009.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-005-1 R1 and CIP-005-1 R1.4

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

DISPOSITION OF VIOLATION
Dated May 16, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
FRCC201000384[1]	**URE_2010_01**
FRCC200900277	**URE_2009_07**

I. VIOLATION INFORMATION[2]

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)[3]
CIP-005-1	**1**		**LOWER**	**N/A**
CIP-005-1	**1**	**1.4**	**LOWER**	**N/A**

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—05 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).

[1] URE self-reported possible violations for CIP-005-1 R1.4 (FRCC201000368) and CIP-005-1 R1.6 (FRCC201000369) on May 17, 2010. FRCC Compliance Enforcement determined these two sub-requirement possible violations should be rolled-up to one R1 violation under a new number (FRCC201000384).
[2] 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.
[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-005-1, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

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 Requirement R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

VIOLATION DESCRIPTION

Second Instance

On May 17, 2010, URE self-reported a possible violation of CIP-005-1 R1 for failure to identify eight digital wall clocks in its Energy Control Center (ECC) as Cyber Assets within the Electronic Security Perimeter (ESP).

On May 6, 2009, eight new Non-Critical Cyber Assets (Non-CCAs), digital wall clocks, were added within URE's ECC ESP, as part of the Energy Management System (EMS) upgrade project but were not placed on URE's Cyber Asset list.

These new devices were added prior to when URE implemented a new change management process for compliance with CIP-003-1 R6.

As a part of URE's CIP Reliability Standards compliance efforts, URE established, documented, and implemented a change control and configuration management process as required by CIP-003-1 R6 to govern the addition, modification, replacement, and removal of Cyber Asset hardware and software prior to URE's July 1, 2009 compliant date for CIP Reliability Standards. This process requires the creation of a change record that includes all relevant Cyber Asset information and the assignment of tasks to secure and test the Cyber Assets and update URE's lists of Critical Cyber Assets and Cyber Assets located within the ESP. To ensure that this new process cannot easily be bypassed when on boarding new Cyber Assets within the ESP, all unused ports within the ECC ESP were disabled. A request must be made within the new process in order to place new devices in service within the ESP.

As Non-CCAs on the energy control network and within the ESP, the eight wall clocks should have been identified pursuant to CIP-005-1 R1.4 and documented pursuant to CIP-005-1 R1.6 on URE's Cyber Asset list.

Although a change request was opened related to the installation of the clocks, the new change control and configuration management process was not yet in place. As a result, these clocks were added to the network, but URE's IT management group was not notified to add the non-critical clocks to the Cyber Asset list. Therefore, the clocks were not appropriately identified and listed as required under CIP-005-1 R1 prior to URE's compliant date on July 1, 2009. These assets were identified through the use of a new network discovery tool on March 25, 2010.

Additionally, as part of URE's response to FRCC staff questions during the April 29, 2010 meeting, URE reviewed its documentation regarding Critical and Non-CCAs on the ECC network beginning July 1, 2009 when CIP-005-1 compliance was required.

This review revealed that, for a portion of that time, an additional CCA (a backup server) on the ECC network was not listed on the URE Cyber Asset list. On June 8, 2009, during a quarterly review and update of the Cyber Asset list this backup server was removed in error by a URE contractor who no longer works at URE. It is unclear why the contractor removed this asset from the Cyber Asset list. The backup server was again placed on the Cyber Asset list on November 6, 2009.

First Instance

On November 5, 2009, URE self-reported a violation of CIP-005-1 R1.4 because it added thirteen new assets to the URE electric ECC network as part of an EMS upgrade. These assets (all EMS-capable personal computers) were added to the URE ECC network via an internal change request. The assets were placed on the ECC protected network, but the assets were not officially listed on URE's Critical Asset listing as provided in URE's internal procedures until October 27, 2009. The

omission was discovered as equipment was being moved from one Physical Security Perimeter (PSP) to another PSP in an effort to reduce the number of individuals with access to URE CCAs. These assets were omitted from the Critical Asset list when the change request was inadvertently closed before all required tasks (including the task of updating the list) were completed.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

FRCC finds that these violations posed a minimal risk and did not pose a serious or substantial risk to the Bulk Power System (BPS) because in both cases the -CCAs were inside a PSP and ESP and no configuration changes were made to these 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)

Second instance: **7/1/09 (date the Standard became mandatory and enforceable for URE) through 3/29/10 (date the clocks were removed from the protected subnet within the ESP; the server was placed back on the Critical Asset list 11/6/09)**

First instance: 7/1/09[5] **(date the Standard became mandatory and enforceable) through 10/27/09 (date the assets were listed on URE's Critical Asset list)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY
R1: **5/17/10**R1.4: **11/5/09**

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

[5] The misclassification occurred on May 19, 2009; however under the NERC CIP implementation plan, Requirement CIP-005-1 R1.4 was not scheduled for "compliant" status until June 30, 2009.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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.	**R1: MIT-09-2720** **R1.4: MIT-09-3346**
DATE SUBMITTED TO REGIONAL ENTITY	**R1: 5/17/10** **R1.4: 11/5/09**[6]
DATE ACCEPTED BY REGIONAL ENTITY	**R1: 7/19/10** **R1.4: 12/16/09**
DATE APPROVED BY NERC	**R1: 8/26/10** **R1.4: 3/1/11**
DATE PROVIDED TO FERC	**R1: 8/26/10** **R1.4: 3/1/11**

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

R1: URE submitted a Self-Report and Mitigation Plan on May 17, 2010 which had listed the violation as CIP-005-1 R1.4 and R1.6. URE later revised the Mitigation Plan on July 16, 2010 to reflect the correct CIP-005-1 R1 violation and revised again on August 19, 2010 to correct the FRCC tracking number.[7]

R1.4: N/A

MITIGATION PLAN COMPLETED YES ☐ NO ☒

EXPECTED COMPLETION DATE	**R1: 9/30/10** **R1.4: 11/30/09**
EXTENSIONS GRANTED	**NONE**
ACTUAL COMPLETION DATE	**R1: 9/28/10** **R1.4: 11/30/09**

[6] URE's Mitigation Plan was dated November 6, 2009; however it was submitted to FRCC on November 5, 2009.

[7] Based on the NERC Sanction Guidelines, FRCC determined the violations of CIP-005-1 R1.4 and R1.6 were "related to a single act or common incidence of non-compliance" for which FRCC would assess "a single aggregate penalty."

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

DATE OF CERTIFICATION LETTER	**R1: 2/7/11** **R1.4: 12/29/09**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**R1: 9/28/10** **R1.4:11/30/09**
DATE OF VERIFICATION LETTER	**R1 and R1.4: 2/7/11**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**R1: 9/28/10** **R1.4: 4/29/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

R1: The URE NERC team has identified the following tasks as part of the action plan to mitigate this finding:

1. Implement change control and configuration management process that should reduce the likelihood of future omissions.

2. Addition of backup server to the Cyber Asset list.

3. Removal of eight wall clocks from the protected subnet within the ESP.

4. Review of ping sweep to verify removal of wall clocks. Ping sweep was reviewed to verify that all eight wall clocks were removed from the ESP.

5. Comparison of Internet Protocol ping sweep (showing all Cyber Assets including the wall clocks and the backup server) to the Cyber Asset list, to verify that all Cyber Assets within the ESP were identified except for the wall clocks.

6. Procure services of independent third party contractor to perform a full physical inventory of Cyber Assets within the URE ESPs.

7. Perform full physical inventory of Cyber Assets within all URE ESPs. Utilizing an independent third party contractor and URE's distributed control system vendor, URE will perform a physical inventory of Cyber Assets within the ESPs within the URE's facilities.

8. Reconcile the physical inventory results to the Cyber Asset list and make any needed corrections.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

R1.4: To prevent future omissions, URE made a change in its management application to ensure that the IT management personnel task of updating the Critical Asset list cannot be closed by any other URE group.

Additionally URE conducted an IP ping sweep of the network and manually compared to the Critical Asset listing to ensure no other Cyber Assets had been omitted.

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)

R1:

A document that shows a change control and configuration management process has been implemented. It also describes the on-boarding of an asset into the database and then the significant and non-significant changes that can be made. Specific for the ESP environment. Signed off by the manager of information security.	**5/15/09**
Addition of backup server to the Cyber Asset List. The item was added and approved. Also reviewed change log	**11/6/09**
Work ticket to remove wall clocks from the secure network to the corporate network and shows closure. Attestation that states 8 digital wall clocks were removed.	**3/29/10**
Ping sweep was reviewed to verify that all eight wall clocks were removed from the ESP. A document that show the wall clocks were not on the ESP network.	**3/31/10**
Cyber Asset List shows no wall clocks. IP Ping Sweep on eight wall clocks were present at the time no longer appear on the CCA list.	**5/6/10**
Purchase Order for third Party contractor for physical inventory project. Purchase order details job scope of work to perform a full physical inventory of physical assets.	**7/30/10**
E-mail notification that work had been completed by vendor. Manager forwarded from Consultants giving project closure details. Work results were provided in Excel format documenting each switch, active ports and connected devices. Secure networks were written in green. Notice of completion from the vendor. Spreadsheet of consultant findings for plant. Spreadsheet of results for ECC.	**9/1/10**

Signed summary document detailed the reconciliation between results of the vendor and physical asset inventory review and the Cyber Asset lists reconciliation. Spreadsheets of items for plants, ECC, etc. Signed list that had to be reconciled (with a total of 38 assets for reconciliation).	**9/30/10**

R1.4:

A document that demonstrates a new change and configuration process developed during May 2009 and rolled out for production and training June 2009	**5/15/09**
Formal training of the new change and configuration process with several employees (including the employee who made the initial error of closing the work order before the final step of adding the assets to the listing was accomplished)	**6/1/09**
Attestation briefly stating the agenda of training held with the employee who made the initial error of closing the work order before the final step of adding the assets to the listing was accomplished	**12/11/09**
Process flow diagram of the new change process that was used during training meeting	**Undated**[8]
Attestation for CCA Reconciliation- This document shows an attestation that a formal manual reconciliation of CCA to IP Ping Sweep has occurred using a change ticket	**10/27/09**
E-mail attestation that the Critical Asset list was updated to now include the 13 Non-CCAs inadvertently left off the list	**12/9/09**
Screenshots of request to change service center (change management system) and actual changes/results- This document shows implementation of task level control and actual changes. System screens were altered so only those operator accounts with "asset management" capability associated with their accounts can close these types of tasks.	**Undated**

[8] A similar flowchart is located in another URE document.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report for CIP-005-1 R1 dated 5/17/10
URE's Self-Report for CIP-005-1 R1.4 dated 11/6/09

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2720 for CIP-005-1 R1 dated 5/17/10
URE's Mitigation Plan MIT-09-2720 for CIP-005-1 R1 revised 8/19/10
URE's Mitigation Plan MIT-09-3346 for CIP-005-1 R1.4 dated 11/5/09

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion for CIP-005-1 R1 dated 2/7/11
URE's Certification of Mitigation Plan Completion for CIP-005-1 R1.4 dated 12/29/09

VERIFICATION BY REGIONAL ENTITY
FRCC's Verification of Mitigation Plan Completion for CIP-005-1 R1 and R1.4 dated 2/7/11