PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

August 31, 2011

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Abbreviated Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP11-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[1] discussed in detail in the Settlement Agreement (Attachment a) and the Disposition Documents attached thereto, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This NOP is being filed with the Commission because Southwest Power Pool Regional Entity (SPP RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SPP RE's determination and findings of the violations of CIP-002-1 Requirement(R)1 and R3, CIP-003-1 R1, CIP-004-1 R2, and CIP-007-1 R1. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of twelve thousand dollars ($12,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions

[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

of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers SPP201000269, SPP201000270, SPP201000273, SPP201000275, SPP201000276 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 24, 2011, by and between SPP RE and URE. The details of the findings and the basis for the penalty are set forth in the Disposition Documents. This NOP filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7, NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
NOC-886	SPP201000269	CIP-002-1	1	Lower[3]	7/1/09 – 8/18/10	12,000
	SPP201000270	CIP-002-1	3	Lower[4]	7/1/08 -8/17/10	
	SPP201000273	CIP-003-1	1	Medium[5]	7/1/08 – 12/30/10	
	SPP201000275	CIP-004-1	2	Lower[6]	7/1/08 – 6/1/10	

[3] CIP-002-1 R1 and R1.2 each are assigned a "Medium" Violation Risk Factor (VRF) and CIP-002-1 R1.2, R1.2.1, R1.2.2, R1.2.3, R1.2.4, R1.2.5, R1.2.6 and R1.2.7 are each assigned a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-002-1 R1 and R1.2 "Lower" VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRFs and on January 27, 2009, the Commission approved the modified "Medium" VRFs. Therefore, the "Lower" VRFs for CIP-002-1 R1 and R1.2 were in effect from June 18, 2007 until January 27, 2009 when the "Medium" VRFs became effective.

[4] CIP-002-1 R3 has a "High" VRF and CIP-002-1 R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-002-1 R3 a "Medium" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "High" VRF and on January 27, 2009, the Commission approved the modified "High" VRF. Therefore, the "Medium" VRF for CIP-002-1 R3 was in effect from June 18, 2007 until January 27, 2009 when the "High" VRF became effective.

[5] CIP-003-1 R1 has a "Medium" VRF; R1.1, R1.2 and R1.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-003-1 R1 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-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[6] 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.

	SPP201000276	CIP-007-1	1	Medium[7]	7/1/08 – 6/24/09	

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

CIP-002-1 R1.1 - OVERVIEW
During a spot check, the SPP RE determined that URE failed to include in its Risk Based Assessment Methodology procedures or evaluation criteria by which system restoration assets are evaluated for purposes of identifying Critical Assets, as required by the Standard.

CIP-002-1 R3.2 - OVERVIEW
During a spot check, the SPP RE determined that URE failed to designate an operator console at its backup control system as a Critical Cyber Asset (CCA). The operator console is essential to the operation of the backup control system because in the event that URE was required to switch over from the primary control system to the backup control system, the console would be utilized to control the Energy Management System (EMS)/Supervisory Control and Data Acquisition (SCADA) system. As such, the console is required by the Standard to be included on the CCA list.

CIP-003-1 R1.1 and R1.2 - OVERVIEW
During a spot check, the SPP RE determined that URE failed to address all of the requirements of CIP-002 through CIP-009, as required by CIP-003-1 R1.1. In addition, URE failed to make the cyber security policy readily available to all personnel with electronic access or unescorted physical access to CCAs as required by CIP-003-1 R1.2. Specifically, the policy was not readily available to the janitorial staff with unescorted physical access or the EMS vendor support staff with electronic access.

CIP-004-1 R2.2.2 - OVERVIEW
During a spot check, the SPP RE determined that URE did not, in its annual cyber security training program for personnel with authorized cyber or authorized unescorted physical access to CCAs, sufficiently address physical access controls utilized by URE to control access to CCAs, as required by CIP-004-1 R2.2.2. The training included one slide addressing the importance of protecting employee access badges from loss or theft, but did not address URE's policies and procedures regarding physical access to CCAs.

CIP-007-1 R1- OVERVIEW
During a spot check, the SPP RE determined that URE did not perform any testing to ensure that significant changes to Cyber Assets within the Electronic Security Perimeter did not adversely affect existing cyber security controls for Microsoft Windows-based servers and workstations located at URE's primary and backup control centers. Before June 24, 2009, URE performed

[7] CIP-007-1 R1 and R1.1 each have a "Medium" VRF; R1.2 and R1.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-007-1 R1.1 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-007-1 R1.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

only functional testing for security patches, software updates, and other significant changes to ensure that the system functioned properly following the change.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[8]

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,[9] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on August 2, 2011. The NERC BOTCC approved the Settlement Agreement, including SPP RE's assessment of a twelve thousand dollar ($12,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. the violations constituted URE 's first occurrence of violation of the subject NERC Reliability Standards;
2. SPP RE reported that URE was cooperative throughout the compliance enforcement process;
3. URE had a compliance program at the time of the violation which SPP RE considered a mitigating factor, as discussed in the Disposition Documents;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. SPP RE determined that the violations did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), as discussed in the Disposition Documents; and
6. SPP RE reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of twelve thousand dollars ($12,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[8] *See* 18 C.F.R. § 39.7(d)(4).
[9] *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).

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.

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 SPP RE and URE executed August 24, 2011, included as Attachment a;

   i. Disposition Document for Common Information, included as Attachment 1 to the Settlement Agreement;

   ii. Disposition Document for CIP-002-1 R1.1 and R3.2, included as Attachment 1a to the Settlement Agreement;

   iii. Disposition Document for CIP-003-1 R1.1 and R1.2, included as Attachment 1b to the Settlement Agreement;

   iv. Disposition Document for CIP-004-1 R2.2.2, included as Attachment 1c to the Settlement Agreement; and

   v. Disposition Document for CIP-007-1 R1, included as Attachment 1d to the Settlement Agreement;

b) SPP RE ’s Public Source Document included as Attachment b;

c) URE’s Mitigation Plan MIT-09-2628 for CIP-002-1 R1.1, included as Attachment c;

d) URE’s Mitigation Plan MIT-09-2629 for CIP-002-1 R3.2, included as Attachment d;

e) URE’s Mitigation Plan MIT-10-2631 for CIP-004-1 R2.2.2, included as Attachment e;

f) URE’s Mitigation Plan MIT-10-2632 for CIP-007-1 R1, included as Attachment f;

g) URE’s Mitigation Plan MIT-08-2630 for CIP-003-1 R1.1 and R1.2, included as Attachment g;

h) URE’s Certification of Mitigation Plan MIT-09-2628 Completion, included as Attachment h;

i) URE’s Certification of Mitigation Plan MIT-09-2629 Completion, included as Attachment i;

j) URE’s Certification of Mitigation Plan MIT-08-2630 Completion, included as Attachment j;

k) URE’s Certification of Mitigation Plan MIT-10-2631 Completion, included as Attachment k;

l) URE’s Certification of Mitigation Plan MIT-10-2632 Completion, included as Attachment l;

m) SPP RE’s Mitigation Plan Completion Notice MIT-09-2628, MIT-09-2629, MIT-08-2631 and MIT-10-2632 Completion, included as Attachment m; and

n) SPP RE’s Mitigation Plan Completion Notice MIT-08-2630 Completion, included as Attachment n.

A Form of Notice Suitable for Publication[10]

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

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 Machelle Smith* Paralegal & SPP RE File Clerk Southwest Power Pool Regional Entity 16101 La Grande, Ste 103 Little Rock, AR 72223 (501) 688-1681 (501) 821-8726 – facsimile spprefileclerk@spp.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	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 Stacy Dochoda* General Manager Southwest Power Pool Regional Entity 16101 La Grande, Ste 103 Little Rock, AR 72223 (501) 688-1730 (501) 821-8726 – facsimile sdochoda.re@spp.org Joe Gertsch* Manager of Enforcement Southwest Power Pool Regional Entity 16101 La Grande, Ste 103 Little Rock, AR 72223 (501) 688-1672 (501) 821-8726 – facsimile jgertsch.re@spp.org

[10] *See* 18 C.F.R. § 39.7(d)(6).

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
Southwest Power Pool Regional Entity

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for Common Information

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment 1

DISPOSITION OF VIOLATIONS[1]

INFORMATION COMMON TO INSTANT VIOLATIONS
Dated August 24, 2011

REGISTERED ENTITY	**NERC REGISTRY ID**	**NOC#**
Unidentified Registered Entity ("URE")	NCRXXXXX	NOC-886

REGIONAL ENTITY
Southwest Power Pool, Regional Entity ("SPP RE")

IS THERE A SETTLEMENT AGREEMENT YES ☒ NO ☐

WITH RESPECT TO THE VIOLATION(S), REGISTERED ENTITY

NEITHER ADMITS NOR DENIES IT (SETTLEMENT ONLY)	YES	☒
ADMITS TO IT	YES	☐
DOES NOT CONTEST IT (INCLUDING WITHIN 30 DAYS)	YES	☐

WITH RESPECT TO THE PROPOSED PENALTY OR SANCTION, REGISTERED ENTITY

ACCEPTS IT	YES	☒
DOES NOT CONTEST IT (INCLUDING WITHIN 30 DAYS)	YES	☐

III. PENALTY INFORMATION

TOTAL PROPOSED PENALTY OR SANCTION OF **$12,000** FOR **FIVE** VIOLATIONS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

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

LIST ANY CONFIRMED OR SETTLED VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

[1]For purposes of this document and attachments hereto, the violations at issue are described as "violations," regardless of their procedural posture and whether they were possible, alleged, or confirmed violations.

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

LIST ANY PRIOR CONFIRMED OR SETTLED VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

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

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

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

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ **NO** ☐

EXPLAIN

URE had a compliance program at the time of the violation which SPP RE considered a mitigating factor.

DOES SENIOR MANAGEMENT TAKE ACTIONS THAT SUPPORT THE COMPLIANCE PROGRAM, SUCH AS TRAINING, COMPLIANCE AS A FACTOR IN EMPLOYEE EVALUATIONS, OR OTHERWISE

YES ☒ NO ☐

EXPLAIN

See above.

EXPLAIN SENIOR MANAGEMENT'S ROLE AND INVOLVEMENT WITH RESPECT TO THE REGISTERED ENTITY'S COMPLIANCE PROGRAM

See above.

(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 (IF THE RESPONSE IS "YES," THE ABBREVIATED NOP FORM MAY NOT BE USED.)

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

(9) ADDITIONAL SUPPORT FOR PROPOSED PENALTY OR SANCTION

OTHER RELEVANT INFORMATION:

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

SETTLEMENT DISCUSSIONS COMMENCED:
DATE: 5/7/2010 OR N/A ☐

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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-002-1 R1.1 and R3.2

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

DISPOSITION OF VIOLATION

Dated August 24, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.
SPP201000269	2010-075
SPP201000270	2010-076

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-002-1	R1	R1.1	Lower[1]	N/A[2]
CIP-002-1	R3	R3.2	Lower[3]	N/A

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

The purpose statement of CIP-002-1 provides in pertinent part: "Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment."

CIP-002-1 R1 provides in pertinent part:

> **R1.** Critical Asset Identification Method — The Responsible Entity[4] shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

[1] CIP-002-1 R1 and R1.2 each are assigned a "Medium" Violation Risk Factor (VRF) and CIP-002-1 R1.2, R1.2.1, R1.2.2, R1.2.3, R1.2.4, R1.2.5, R1.2.6 and R1.2.7 are each assigned a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-002-1 R1 and R1.2 "Lower" VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRFs and on January 27, 2009, the Commission approved the modified "Medium" VRFs. Therefore, the "Lower" VRFs for CIP-002-1 R1 and R1.2 were in effect from June 18, 2007 until January 27, 2009 when the "Medium" VRFs became effective.

[2] At the time of the violation, no VSLs were in effect for CIP-002-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[3] CIP-002-1 R3 has a "High" VRF and CIP-002-1 R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-002-1 R3 a "Medium" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "High" VRF and on January 27, 2009, the Commission approved the modified "High" VRF. Therefore, the "Medium" VRF for CIP-002-1 R3 was in effect from June 18, 2007 until January 27, 2009 when the "High" VRF became effective.

[4] Within the text of Standard CIP-002, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC and Regional Reliability Organizations.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.
R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.
R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.
R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.
R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.
R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.
R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

(Footnote added)

CIP-002-1 R3 provides:

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples are control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

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

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

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

VIOLATION DESCRIPTION

SPP201000269: During a spot check, the SPP RE discovered that URE's Risk Based Assessment Methodology (RBAM) was not compliant with CIP-002-1 R1.1, which requires a documented RBAM that includes the procedures and evaluation criteria for identifying Critical Assets. CIP-002-1 R1.2.1 through R1.2.7 list the categories of assets that must be considered in the RBAM. CIP-002-1 R1.2.4 requires consideration of "[s]ystems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration." URE's RBAM failed to include procedures or evaluation criteria by which system restoration assets are evaluated for purposes of identifying Critical Assets.

URE's RBAM focused on the performance of a steady state power flow analysis and a transient stability analysis. Both of these analyses are predicated upon an energized transmission system and are not applicable to an assessment of assets that are used to restore URE from a fully de-energized state without assistance from neighboring entities. The RBAM referenced R1.2.4 and provided that system restoration facilities were to be evaluated for inclusion on the Critical Asset list, but provided no basis or criteria for URE to use in determining whether a particular system restoration asset should be deemed a Critical Asset.

SPP201000270: During the spot check, SPP RE discovered that URE was not in compliance with CIP-002-1 R3. Specifically, URE failed to designate an operator console at its backup control system as a Critical Cyber Asset (CCA). The console would be utilized to control the Energy Management System (EMS)/ Supervisory Control and Data Acquisition (SCADA) system in the event that URE were required to switch over from the primary control system to the backup control system. As a result, the operator console is essential to the operation of the backup control system, which is a Critical Asset, and therefore is required by CIP-002-1 R3 to be included on the CCA list.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

SPP201000269: SPP RE has determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. URE's RBAM stated that restoration resources were considered for inclusion on the Critical Asset list, even though proper evaluation criteria for these resources were not set out in the RBAM. Proper criteria existed for all other asset classes required to be considered under CIP-002-1 R1. Upon its application of a revised RBAM that included evaluation criteria for restoration resources, URE identified no CCAs associated with the restoration resources that it identified as Critical Assets.

SPP201000270: SPP RE has determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. Although the console was not included on the CCA list, it was protected by restricted physical and electronic access. The console was located in an area with 24 hour, seven days a week operations personnel on duty.

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)

SPP201000269: 7/1/09 through 8/18/10 (date the mitigation plan was successfully completed)

SPP201000270: 7/1/08 through 8/17/10 (date the mitigation plan was successfully completed)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY
Spot Check

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

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO. MIT-09-2628 (SPP201000269)

DATE SUBMITTED TO REGIONAL ENTITY	6/30/2010
DATE ACCEPTED BY REGIONAL ENTITY	6/30/2010
DATE APPROVED BY NERC	7/28/2010
DATE PROVIDED TO FERC	7/28/2010

IDENTIFY AND EXPLAIN VERSIONS THAT WERE REJECTED, IF APPLICABLE N/A

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	8/31/2010
EXTENSIONS GRANTED	N/A
ACTUAL COMPLETION DATE	8/18/2010
DATE OF CERTIFICATION LETTER	8/26/2010
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	8/26/2010
DATE OF VERIFICATION LETTER	10/01/2010
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	8/18/2010[5]

MITIGATION PLAN NO. MIT-08-2629 (SPP201000270)

DATE SUBMITTED TO REGIONAL ENTITY	6/30/2010
DATE ACCEPTED BY REGIONAL ENTITY	6/30/2010
DATE APPROVED BY NERC	7/28/2010
DATE PROVIDED TO FERC	7/28/2010

IDENTIFY AND EXPLAIN VERSIONS THAT WERE REJECTED, IF APPLICABLE N/A

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	8/31/2010
EXTENSIONS GRANTED	N/A
ACTUAL COMPLETION DATE	8/17/2010

[5] Although the Verification letter states that the Mitigation Plan was complete as of August 26, 2010, the Mitigation Plan was actually complete on August 18, 2010.

DATE OF CERTIFICATION LETTER	8/26/2010
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	8/26/2010
DATE OF VERIFICATION LETTER	10/01/2010
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	8/17/2010[6]

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

SPP201000269: URE revised its RBAM to require that the Critical Asset list include blackstart generators and substations in the black-start cranking path that are necessary to restore proper operational integrity to the system as provided in URE's blackstart plan. Upon application of the new RBAM, URE identified a blackstart generator and a 138 kV substation as Critical Assets.

SPP201000270: URE updated its list of CCAs as well as its backup control system network layout drawing to include the operator console at the backup control system as a CCA. URE also redefined its physical and electronic security perimeters to ensure that the backup control system operator console is contained within both.

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED)

SPP201000269:

1. URE's Methodology for Critical Asset and Critical Cyber Asset Identification

2. Critical Asset Identification worksheet

SPP201000270:

1. URE's backup control system CCA list

2. URE's physical layout

3. URE's backup control system network diagram showing Electronic Security Perimeter.

[6] Although the Verification letter states that the Mitigation Plan was complete as of August 27, 2010, the Mitigation Plan was actually complete on August 17, 2010.

EXHIBITS:

SOURCE DOCUMENT
SPP RE's Public Source Document

MITIGATION PLAN
URE's Mitigation Plan MIT-09-2628 (CIP-002-1 R1)

URE's Mitigation Plan MIT-08-2629 (CIP-002-1 R3)

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan MIT-09-2628 (CIP-002-1 R1) Completion

URE's Certification of Mitigation Plan MIT-08-2629 (CIP-002-1 R3) Completion

VERIFICATION BY REGIONAL ENTITY
SPP RE's Mitigation Plan Completion Notice

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-003-1 R1.1 and R1.2

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

DISPOSITION OF VIOLATION

Dated August 24, 2011

NERC TRACKING NO.	**REGIONAL ENTITY TRACKING NO.**
SPP201000273	2010-079

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-003-1	R1	R1.1, R1.2	Medium[1]	N/A[2]

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

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

CIP-003-1 R1 provides in pertinent part:

> **R1.** Cyber Security Policy — The Responsible Entity[3] shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:
>
> > **R1.1.** The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
> >
> > **R1.2.** The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

(Footnote added)

---

[1] CIP-003-1 R1 has a "Medium" Violation Risk Factor (VRF); R1.1, R1.2 and R1.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-003-1 R1 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-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[2] At the time of the violation, no VSLs were in effect for CIP-003-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[3] Within the text of Standard CIP-003, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC and Regional Reliability Organizations.

VIOLATION DESCRIPTION

During a spot check, the SPP RE discovered that URE was not in compliance with CIP-003-1 R1. URE's cyber security policy failed to address all of the requirements of CIP-002 through CIP-009 as required by CIP-003-1 R1.1. For example, R1 of both versions of CIP-002 was not addressed in URE's cyber security policy, nor was R4 of both versions of CIP-003. The cyber security policy properly addressed R2.3 of CIP-003-1; however, at the time of the violation, the policy was not updated to address the requirement as modified by Version 2 of the Standard.

Additionally, URE failed to make the cyber security policy readily available to all personnel with electronic access or unescorted physical access to Critical Cyber Assets, as required by CIP-003-1 R1.2. Specifically, the policy was not readily available to the janitorial staff with unescorted physical access or the Energy Management System (EMS) vendor support staff with electronic access.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

SPP RE has determined that the violation posed a minimal and did not pose a serious or substantial risk to the reliability of the Bulk Electric System. Although URE did not have a comprehensive cyber security policy that was compliant with CIP-003-1 R1, it did have cyber security procedures and a cyber security training program in place. URE also had a compliance policy indicating management's commitment to comply with the reliability standards. Further, although a cyber security policy was not made readily available to janitorial and EMS support staff, these individuals received personnel risk assessments and cyber security training, and their access rights were maintained pursuant to CIP-004.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S)
7/01/2008 through12/30/2010 (date the mitigation plan was successfully completed)

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY Spot Check

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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** ☒

MITIGATION INFORMATION FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	MIT-08-2630
DATE SUBMITTED TO REGIONAL ENTITY	6/30/2010
DATE ACCEPTED BY REGIONAL ENTITY	6/30/2010
DATE APPROVED BY NERC	8/12/2010
DATE PROVIDED TO FERC	8/12/2010

IDENTIFY AND EXPLAIN VERSIONS THAT WERE REJECTED, IF APPLICABLE[4] N/A

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	12/30/2010
EXTENSIONS GRANTED	N/A
ACTUAL COMPLETION DATE	12/30/2010
DATE OF CERTIFICATION LETTER	12/30/10
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	12/30/10
DATE OF VERIFICATION LETTER	1/19/11
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	12/30/10

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE revised its Cyber Security Policy to address all requirements of CIP-002 through CIP-009, including provision for emergency situations. URE also made the policy readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets, including vendors and contractors.

[4] The mitigation plan was originally submitted on June 30, 2010 and was accepted; however, two amendments were made. The mitigation plan was amended on July 30, 2010 to conform to the three month rule regarding milestones. A second amendment was made when a milestone activity deadline was moved from September 30, 2010 to December 31, 2010; however, the completion date of the mitigation plan was not modified as a result of this amendment. So while the original mitigation plan was never rejected, there were two subsequent versions due to the amendments.

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

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED)

1. URE's revised Cyber Security Policy
2. Email providing Cyber Security Policy to vendor
3. List of policies and procedure for Janitors / Guards / Vendors

EXHIBITS:

SOURCE DOCUMENT
SPP RE's Public Source Document

MITIGATION PLAN
URE's Mitigation Plan MIT-08-2630

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

VERIFICATION BY REGIONAL ENTITY
SPP RE's Mitigation Plan Completion Notice

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-004-1 R2.2.2

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment 1c

DISPOSITION OF VIOLATION

Dated August 24, 2011

NERC TRACKING NO.	**REGIONAL ENTITY TRACKING NO.**
SPP201000275	2010-081

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-004-1	R2.2	R2.2.2	Lower[1]	N/A[2]

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

The purpose statement of CIP-004-1 provides in pertinent part: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-004-1 R2 provides in pertinent part:

> **R2.** Training – The Responsible Entity[3] shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
>
> …
>
> **R2.2.** Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-1, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:
>
> …

[1] 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.

[2] At the time of the violation, no VSLs were in effect for CIP-004-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

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

R2.2.2. Physical and electronic access controls to Critical Cyber Assets.

(Footnote added)

VIOLATION DESCRIPTION

During a spot check conducted, the SPP RE discovered that URE's annual cyber security training program for personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCA) did not sufficiently address physical access controls utilized by URE to control access to CCAs as required by CIP-004-1 R2.2.2. The training included one slide addressing the importance of protecting employee access badges from loss or theft, but did not address URE's policies and procedures regarding physical access to CCAs.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

SPP RE has determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the Bulk Power System. The training provided to URE employees was comprehensive in regards to all other required items besides physical access controls to CCAs. The training did have one slide regarding the protection of employee access badges from loss or theft, which conveyed to personnel the importance of ensuring that only approved individuals be allowed physical access to particular locations and facilities. Further, URE's procedure was available to all employees.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S)
7/1/08 through 6/1/10 (date the mitigation plan was successfully completed)

DATE REPORTED TO REGIONAL ENTITY Spot Check

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

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

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	MIT-10-2631
DATE SUBMITTED TO REGIONAL ENTITY	6/30/2010
DATE ACCEPTED BY REGIONAL ENTITY	6/30/2010
DATE APPROVED BY NERC	7/28/2010
DATE PROVIDED TO FERC	7/28/2010

IDENTIFY AND EXPLAIN VERSIONS THAT WERE REJECTED, IF APPLICABLE N/A

MITIGATION PLAN COMPLETED	YES	☒	NO	☐

EXPECTED COMPLETION DATE	8/31/2010
EXTENSIONS GRANTED	N/A
ACTUAL COMPLETION DATE	6/1/2010
DATE OF CERTIFICATION LETTER	7/16/2010
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	6/1/2010
DATE OF VERIFICATION LETTER	10/1/2010
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	6/1/2010[4]

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE revised its online cyber security training program for 2010 to include information regarding URE's policies, access controls, and procedures relating to physical access to CCAs. The revised 2010 training was delivered to all personnel who have electronic access and unescorted physical access to CCAs.

[4] The Mitigation Plan Completion Notice incorrectly states that the mitigation plan was complete on April 23, 2010. The actual date of completion is June 1, 2010.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED)

1. URE training slides
2. List of recipients of URE's 2010 cyber security training
3. URE unescorted physical access list
4. URE electronic access list

EXHIBITS:

SOURCE DOCUMENT
SPP RE's Public Source Document

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2631

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

VERIFICATION BY REGIONAL ENTITY
SPP RE's Mitigation Plan Completion Notice

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition Document for CIP-007-1 R1

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachment 1d

DISPOSITION OF VIOLATION

Dated August 24, 2011

NERC TRACKING NO.	**REGIONAL ENTITY TRACKING NO.**
SPP201000276	2010-082

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	R1		Medium[1]	N/A[2]

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

The purpose statement of CIP-007-1 provides in pertinent part:

> 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). 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 requires in pertinent part:**
>
> **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

[1] CIP-007-1 R1 and R1.1 each have a "Medium" VRF; R1.2 and R1.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-007-1 R1.1 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-007-1 R1.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[2] At the time of the violation, no VSLs were in effect for CIP-007-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[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.

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.

VIOLATION DESCRIPTION

During a spot check, the SPP RE discovered that prior to June 24, 2009, URE did not perform any testing to ensure that significant changes to Cyber Assets within the Electronic Security Perimeter (ESP) did not adversely affect existing cyber security controls for Microsoft Windows-based servers and workstations located at URE's primary and backup control centers. Before June 24, 2009, URE performed only functional testing for security patches, software updates, and other significant changes to ensure that that the system functioned properly following the change.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

SPP RE has determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the Bulk Power System. These servers and workstations (assets) are not part of the Energy Management System (EMS), are primarily used for Inter-Control Center Communications Protocol data exchange, and do not connect to the Internet. Moreover, although URE did not perform all of the required testing, it performed functional testing to ensure that the system functioned properly following the change.

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

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

DURATION DATE(S): 7/1/08 through 6/24/09 (date the mitigation plan was successfully completed)

DATE DISCOVERY BY OR REPORTED TO REGIONAL ENTITY
Spot Check

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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** ☒

MITIGATION INFORMATION FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	MIT-10-2632
DATE SUBMITTED TO REGIONAL ENTITY	6/30/2010
DATE ACCEPTED BY REGIONAL ENTITY	6/30/2010
DATE APPROVED BY NERC	7/28/2010
DATE PROVIDED TO FERC	7/28/2010

IDENTIFY AND EXPLAIN VERSIONS THAT WERE REJECTED, IF APPLICABLE N/A

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	8/31/2010
EXTENSIONS GRANTED	N/A
ACTUAL COMPLETION DATE	6/24/2009

DATE OF CERTIFICATION LETTER	7/16/2010
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	6/24/2010[4]

DATE OF VERIFICATION LETTER	10/1/2010
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	6/24/2009[5]

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

At the time of the spot check, URE had already implemented a procedure to ensure that cyber security controls suffer no adverse effects as a result of the introduction of new or significant changes to existing Cyber Assets within the ESP. The procedure involves a comparison of open ports and services from before and after the change. URE was in violation of CIP-007-1 R1 for less than one year.

[4] URE's certification incorrectly provides that the mitigation plan was complete as of July 24, 2010 rather than June 24, 2009.
[5] The Mitigation Plan Completion Notice incorrectly states that the mitigation plan was completed on July 24, 2009, rather than the correct date of June 24, 2009.

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

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN OR MILESTONES (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED)

1. Cyber Security management policy

EXHIBITS:

SOURCE DOCUMENT
SPP RE's Public Source Document

MITIGATION PLAN
URE's Mitigation Plan MIT-10-2632

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

VERIFICATION BY REGIONAL ENTITY
SPP RE's Mitigation Plan Completion Notice