PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 26, 2011

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

Re: NERC Full 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 Notice of Penalty[1] regarding Unidentified Registered Entity (URE), 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]

These violations[3] were discovered by and disclosed to Reliability*First* in several ways. First, Reliability*First* conducted a Spot Check to assess URE's compliance with thirteen enforceable requirements of the CIP Reliability Standards and discovered violations of CIP-002-1 Requirement (R) 1, CIP-003-1 R1.1, CIP-004-1 R2.1, R3 and R4, CIP-007-1 R1, CIP-008-1 R1 and CIP-009-1 R1. Immediately following the Spot Check, URE began creating and implementing a revised, comprehensive CIP program. URE self-certified non-compliance with CIP-003-1 R4, R5 and R6, CIP-005-1 R1,[4] R2, R3 and R5, CIP-006-1 R1 and R3, CIP-007-1 R2, R3, R4, R5, R6, R7 and R9, and CIP-009-1 R3 and R4.[5]

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2010). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] 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.

[4] The Settlement Agreement incorrectly states that the violation of CIP-005-1 R1 was discovered at the Spot Check.

[5] URE also self-certified non-compliant with CIP-005-1 R4, CIP-007-1 R8, CIP-008-1 R2 and CIP-009-1 R2 and R5.

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

Based on the results from the Spot Check and its continued interaction with URE, Reliability*First* determined that additional monitoring of URE was appropriate, including an unscheduled compliance audit approximately six months after the conclusion of the Spot Check. Therefore, Reliability*First* conducted an unscheduled compliance audit (Unscheduled Audit) to assess URE's compliance with all the requirements of the CIP Reliability Standards. At the Unscheduled Audit, Reliability*First* observed substantial improvements to URE's CIP compliance program. The Unscheduled Audit revealed no additional violations, but Reliability*First* did gather additional information regarding the scope and duration of the previously discovered and reported violations.

This Notice of Penalty is being filed with the Commission because Reliability*First* and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from Reliability*First*'s determination and findings of the enforceable violations of CIP-002-1 R1, CIP-003-1 R1, R4, R5, R6, CIP-004-1 R2, R3, R4, CIP-005-1 R1, R2, R3, R5, CIP-006-1 R1, R3, CIP-007-1 R1, R2, R3, R4, R5, R6, R7, R9, CIP-008-1 R1, CIP-009-1 R1, R3, and R4. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of seventy thousand dollars ($70,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers RFC200900208, RFC200900209, RFC201000345, RFC201000346, RFC201000347, RFC200900210, RFC200900211, RFC200900212, RFC201000348, RFC201000349, RFC201000350, RFC201000352, RFC201000353, RFC201000354, RFC200900213, RFC201000355, RFC201000356, RFC201000369, RFC201000357, RFC201000370, RFC201000358, RFC201000360, RFC200900214, RFC200900215, RFC201000363, and RFC201000364 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement effective November 22, 2010, by and between Reliability*First* and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty 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 (2007), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty ($)
Reliability*First*	Unidentified	729	RFC200900208	CIP-002-1[6]	1	Medium[7]	70,000

[6] Reliability*First* initially discovered the violations while the first version of the CIP Reliability Standards was effective. The second version of the CIP Reliability Standards became effective April 1, 2010 and Version three became effective on October 1, 2010. As a result, some of the violations span both or all three versions of the CIP Reliability Standards.

	Registered Entity		RFC200900209	CIP-003-1	1	Medium[8]	
			RFC201000345	CIP-003-1	4	Medium	
			RFC201000346	CIP-003-1	5	Lower	
			RFC201000347	CIP-003-1	6	Lower	
			RFC200900210	CIP-004-1	2	Medium[9]	
			RFC200900211	CIP-004-1	3	Medium[10]	
			RFC200900212	CIP-004-1	4	Lower[11]	
			RFC201000348	CIP-005-1	1	Medium	
			RFC201000349	CIP-005-1	2	Medium	
			RFC201000350	CIP-005-1	3	Medium	
			RFC201000352	CIP-005-1	5	Lower	
			RFC201000353	CIP-006-1	1	Medium[12]	
			RFC201000354	CIP-006-1	3	Medium	
			RFC200900213	CIP-007-1	1	Medium	
			RFC201000355	CIP-007-1	2	Medium	
			RFC201000356	CIP-007-1	3	Lower	
			RFC201000369	CIP-007-1	4	Medium[13]	
			RFC201000357	CIP-007-1	5	Lower	

[7] When NERC filed Violation Risk Factors (VRF) it originally assigned CIP-002-1 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-002-1 R1 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

[8] 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.

[9] 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.

[10] CIP-004-1 R3 has a "Medium" Violation Risk Factor (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.

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

[12] When NERC filed VRFs it originally assigned CIP-006-1 R1.5 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 February 2, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-006-1 R1.5 was in effect from June 18, 2007 until February 2, 2009, when the "Medium" VRF became effective.

[13] When NERC filed VRFs it originally assigned CIP-007-1 R4 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 February 2, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-007-1 R4 was in effect from June 18, 2007 until February 2, 2009, when the "Medium" VRF became effective.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

			RFC201000370	CIP-007-1	6	Lower	
			RFC201000358	CIP-007-1	7	Lower	
			RFC201000360	CIP-007-1	9	Lower	
			RFC200900214	CIP-008-1	1	Lower	
			RFC200900215	CIP-009-1	1	Medium	
			RFC201000363	CIP-009-1	3	Lower	
			RFC201000364	CIP-009-1	4	Lower	

CIP-002-1 R1

The purpose statement of CIP-002-1 provides in pertinent part:

> NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
>
> ****
>
> 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[14] shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.
>
> R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

(Footnote added.)

CIP-002-1 R1 has a "Medium" Violation Risk Factor (VRF).

Reliability*First* determined that URE had a violation of CIP-002-1 R1 because during the Spot Check, no documentation describing its risk-based assessment methodology was available for the compliance period of July 1, 2008 through July 14, 2008. URE's initial cyber security policy was not effective until July 15, 2008. Although URE asserted that the policy was actually in effect on July 1, 2008, Reliability*First* found these assertions insufficient to show URE's compliance for the first fourteen days of the compliance period.

Reliability*First* determined the duration of the violation to be from July 1, 2008, the date on which URE was required to comply with CIP-002-1 R1 as a Table 1 entity for its System Control Center,[15] through April 12, 2010, when URE completed its Mitigation Plan.

[14] 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.
[15] All of URE's Critical Cyber Assets are housed at its System Control Center.

CIP-003-1 R1, R4, R5 and R6

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 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
>
> R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
>
> > R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
> >
> > R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
> >
> > R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.
>
> R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
>
> > R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
> >
> > > R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.
> > >
> > > R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

CIP-003-1 R1 and R4 have a "Medium" VRF; R5 and R6 have a "Lower" VRF.

At the Spot Check, Reliability*First* discovered a violation of CIP-003-1 R1 where URE failed to address the following requirements of CIP-002-1 through CIP-009-1 in its cyber security policy: CIP-005-1 R1, R2, R3, R4 and R5; CIP-007-1 R1, R2, R3, R6, R7 and R8; CIP-008-1 R2; and CIP-009-1 R2, R3, R4 and R5. Reliability*First* reviewed two successive versions of URE's cyber security policy, both of which were effective during the time period covered by the Spot Check. Reliability*First* determined that both versions of the policy failed to contain provisions for emergency situations in accordance with CIP-003-1 R1.1. URE sought to correct the deficiencies found by the Spot Check team by implementing a new cyber security policy. Believing its new cyber security policy to be fully compliant with CIP-003-1 R1, URE self-certified "Auditably Compliant" to CIP-003-1 R1 on February 1, 2010. At the Unscheduled Audit, Reliability*First* discovered a continuing violation of CIP-003-2 R1.1 because URE's revised cyber security policy contained a statement permitting URE to not take the actions specified in certain requirements and accept any risks associated with that decision. The Commission stated that statements in a cyber security policy allowing entities to accept risks would render the policy non-compliant upon the effective date of Version 2 of the CIP Reliability Standards, April 1, 2010.[16] Reliability*First* determined that URE's inclusion of a statement accepting risk meant that URE's cyber security policy did not adequately address the requirements of CIP-002 through CIP-009, as required by CIP-003-2, R1.1. URE violated CIP-003-1 R1.1 by failing to implement a cyber security policy addressing the requirements in Standards CIP-002 through CIP-009, including a provision for emergency situations. Additionally, Reliability*First* determined that URE violated CIP-003-2 R1.1 by including a statement accepting risk in its cyber security policy.

URE also self-certified "Substantially Compliant" to CIP-003-1 R4. URE did not implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets; resulting in a failure to document the protections afforded the types of information

[16] *See* 122 FERC ¶ 61,040, at P.150.

listed in CIP-003-1 R4.1. URE also failed to classify information based on the sensitivity of the Critical Cyber Asset information in accordance with CIP-003-1 R4.2. Finally, URE did not implement and document an information protection program which resulted in its failure to assess annually its adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment in accordance with CIP-003-1 R4.3.

URE also self-certified "Substantially Compliant" to CIP-003-1 R5. URE failed to: maintain a list of personnel responsible for authorizing access in accordance with CIP-003-1 R5.1; review its access privileges to protected information in accordance with CIP-003-1 R5.2; and assess and document at least annually its processes for controlling access privileges to protected information in accordance with CIP-003-1 R5.3.

URE also self-certified "Substantially Compliant" to CIP-003-1 R6. URE did not establish and document a process of change control and configuration management for adding, modifying, or removing Critical Cyber Asset hardware or software, and implementing supporting configuration management activities to identify, control, and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

Reliability*First* determined the duration of the CIP-003-1 R1 violation to be from July 1, 2008, the date on which URE was required to comply with CIP-003-1 R1 as a Table 1 Entity for its System Control Center, through October 29, 2010, when URE completed its Mitigation Plan.

Reliability*First* determined the duration of the CIP-003-1 R4, R5, and R6 violation to be from July 1, 2009, the date on which URE was required to comply with CIP-003-1 R4, R5 and R6 as a Table 1 entity for its System Control Center, through October 29, 2010, when URE completed its Mitigation Plan.

CIP-004-1 R2, R3 and R4

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 provides in pertinent part:

> R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
>
> R2.1. 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.

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.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

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

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

CIP-004-1 R2 and R3 each has a "Medium" VRF and R4 has a "Lower" VRF.

At the Spot Check, Reliability*First* discovered a violation of CIP-004-1 R2 by concluding that URE failed to train 32 individuals with authorized cyber or authorized unescorted physical access to Critical Cyber Assets within ninety days of those individuals' access authorizations. All of the 32 individuals maintained authorized unescorted physical access to URE's control center and the Critical Cyber Assets contained therein, while nine of the 32 maintained cyber access to Critical Cyber Assets. The 32 individuals were all trained as of July 31, 2009.[17]

At the Spot Check, Reliability*First* discovered a violation of CIP-004-1 R3 by concluding that URE failed to complete personnel risk assessments for 32 individuals with access to Critical Cyber Assets within 30 days of granting such access. As to ten of these individuals, URE was delayed in performing personnel risk assessments because it had to resolve bargaining unit issues before performing them. As to the other 22 individuals, URE misunderstood CIP-004-1 R3 as requiring completion of personnel risk assessments within 30 days of the cyber security policy becoming effective. As of February 9, 2009, URE completed personnel risk assessments on the 32 individuals at issue.

At the Spot Check, Reliability*First* discovered a violation of CIP-004-1 R4 by concluding that URE failed to include 20 individuals with "passcard" access to Critical Cyber Assets on its list of personnel with authorized cyber or authorized unescorted physical access because URE

[17] These 32 individuals had access without being trained for various durations ranging from 45 days to 381 days.

mistakenly considered these individuals as having escorted physical access to Critical Cyber Assets. Reliability*First* also determined that URE failed to train these 20 individuals as required by CIP-004-1 R2 and did not perform personnel risk assessments as required by CIP-004-1 R3. Since discovering this issue, URE determined that only four of these 20 individuals required access to Critical Cyber Assets, and URE trained and performed personnel risk assessments on these four individuals. URE revoked access for the other 16 individuals.

Reliability*First* determined the duration of the violations to be from July 1, 2008, the date on which URE was required to comply with CIP-004-1 as a Table 1 entity for its System Control Center, through April 12, 2010, when URE completed its Mitigation Plan. Reliability*First* noted that URE completed all the necessary training and personnel risk assessments to effectuate compliance with CIP-004-1 R2 and R3 as of July 31, 2009.

CIP-005-1 R1, R2, R3 and R5

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 access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."

CIP-005-1 states in pertinent part:

> R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> > R1.1. 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).
> >
> > * * * * *
> >
> > R1.3. 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.
>
> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> * * * * *

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

* * * * *

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

* * * * *

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

CIP-005-1 R1, R2, and R3 have a "Medium" VRF and R5 has a "Lower" VRF.
URE self-certified "Substantially Compliant" to CIP-005-1 R1.[18] URE did not identify access points to an Electronic Security Perimeter in accordance with CIP-005-1 R1. Additionally, URE failed to consider end points of communication links within an Electronic Security Perimeter as access points to the Electronic Security Perimeter in accordance with CIP-005-1 R1.3, and further, URE failed to identify and protect certain non-critical Cyber Assets, in this case printers, in accordance with CIP-005-1 R1.4. At the Unscheduled Audit, Reliability*First* discovered that URE failed to identify an externally connected network switch that terminates within an Electronic Security Perimeter as an access point to an Electronic Security Perimeter in accordance with CIP-005-1 R1.1. Additionally, URE failed to consider the end point of a router within an Electronic Security Perimeter connecting two discrete Electronic Security Perimeters as an access point in accordance with CIP-005-1 R1.3.

URE self-certified "Substantially Compliant" to CIP-005-1 R2. Although URE did produce evidence demonstrating that it does have some technical controls in place at electronic access points to the Electronic Security Perimeters,[19] URE failed to sufficiently control electronic access to Critical Cyber Assets as follows: (i) identify only those ports and services required for operating and monitoring Cyber Assets within an Electronic Security Perimeter in accordance with CIP-005-1 R2.2; (ii) implement strong procedural or technical controls at access points in accordance with CIP-005-1 R2.4; (iii) document processes for access request and authorization, authentication methods, and review of authorization rights in accordance with CIP-005-1 R2.5; and (iv) display an "appropriate use banner" in accordance with CIP-005-1 R2.6. Additionally, based on findings from the Unscheduled Audit, URE failed to show that its open ports and services are only those required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, as required by CIP-005-1 R2.2.

URE self-certified "Substantially Compliant" to CIP-005-1 R3. URE did not address monitoring electronic access and did not create electronic or manual processes for monitoring and logging access at access points in accordance with CIP-005-1 R3. Additionally, URE failed to create monitoring processes for detecting and alerting for attempted or actual unauthorized accesses

[18] The settlement agreement incorrectly states that the CIP-005-1, R1 alleged violation was discovered during the Spot Check.
[19] URE blocks all remote access with the exception of communication between Electronic Security Perimeters and protects access points to its Electronic Security Perimeters using firewalls.

with appropriate notification to designated response personnel in accordance with CIP-005-1 R3.2.

URE self-certified "Substantially Compliant" to CIP-005-1 R5. URE did not review, update, and maintain all documentation to support compliance with the requirements of CIP-005-1. Specifically, URE: (i) failed to generate and retain electronic access logs for at least 90 calendar days in accordance with CIP-005-1 R5.2; and (ii) failed to document changes resulting from modifications to the network or controls within 90 calendar days of the changes being completed in accordance with CIP-005-1 R5.3. URE did maintain and review documentation of its Electronic Security Perimeter as part of its Cyber Security Policy.

Reliability*First* determined the duration of the violations to be from July 1, 2009, the date on which URE was required to comply with CIP-005-1 as a Table 1 entity for its System Control Center, through October 29, 2010, when URE completed its Mitigation Plan.

CIP-006-1 R1 and R3

The purpose statement of CIP-006-1 provides in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."

In pertinent part, CIP-006-1 R1 states:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> * * * * *
>
> R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.
>
> R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).
>
> R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
>
> R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.
>
> * * * * *
>
> R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not

limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

* * * * *

R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:

R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

CIP-006-1 R1 and R3 have a "Medium" VRF.

URE self-certified "Substantially Compliant" to CIP-006-1 R1. URE did not have in place a physical security plan that addressed all the elements of CIP-006-1 R1. Specifically, URE did not have: (i) documented processes to identify all access points through each Physical Security Perimeter in accordance with CIP-006-1 R1.2; (ii) documented processes and procedures to monitor physical access to the perimeters in accordance with CIP-006-1 R1.3; (iii) documented procedures for the appropriate use of physical access controls, including response to loss and prohibition of inappropriate use of physical access controls in accordance with CIP-006-1 R1.4; (iv) documented procedures for reviewing access authorization requests and revocation of access authorization in accordance with CIP-006-1 R1.5; and (v) documented processes for updating the physical security plan within 90 calendar days of any physical security system redesign or reconfiguration in accordance with CIP-006-1 R1.7. URE also failed to afford all the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009 to Cyber Assets used in the access control and monitoring of the Physical Security Perimeters as required by CIP-006-1 R1.8. Finally, although required by the physical security plan provisions of URE's cyber security policy, URE failed to

ensure that these physical security plan provisions were reviewed at least annually in accordance with CIP-006-1 R1.9.

URE self-certified "Substantially Compliant" to CIP-006-1 R3. URE did not document and implement technical and procedural controls for monitoring physical access at all access points to Physical Security Perimeters twenty-four hours a day, seven days a week. Additionally, URE did not review unauthorized access attempts. For the duration of the violation, URE recognized three distinct Physical Security Perimeters and six total access points to these Physical Security Perimeters. URE did have technical controls, such as motion detecting alarms, in place to monitor access to these Physical Security Perimeters, however, URE failed to document these controls.

Reliability*First* determined the duration of the violation to be from July 1, 2009 the date on which URE was required to comply with CIP-006-1 as a Table 1 entity for its Control Center, through April 12, 2010, when URE completed its Mitigation Plan.

CIP-007-1 R1, R2, R3, R4, R5, R6, R7 and R9

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

CIP-007-1 R1 states 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 cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
>
> > R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.
> >
> > R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
> >
> > R1.3. The Responsible Entity shall document test results.
>
> R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

* * * * *

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

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and “special” characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

> R7. Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
>
> * * * * *
>
> R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.

CIP-007-1 R1, R2, and R4 have a "Medium" VRF,[20] R3, R5, R6, R7, and R9 have a "Lower" VRF.

At the Spot Check, Reliability*First* discovered a violation of CIP-007-1 R1 by concluding that URE failed to test for any adverse effects on cyber security controls caused by new or changed Cyber Assets. Reliability*First* also discovered an instance in which URE installed a server within an Electronic Security Perimeter. URE failed to show that it tested the server in a manner that minimized the impact to the production environment and in a manner that reflected the production environment in accordance with CIP-007-1 R1.1. Furthermore, although URE documented that limited testing occurred, URE failed to document the results of its testing in accordance with CIP-007-1 R1.3.

URE self-certified "Substantially Compliant" to CIP-007-1 R2. URE had not established, documented, and implemented a process to ensure that only those ports and services required for normal and emergency operations were enabled as required by CIP-007-1 R2. URE also determined that it had failed to create documentation identifying the critical ports and services as required for CIP-007-1 R2. At the Unscheduled Audit, Reliability*First* found that URE had established and documented processes, contained in various documents, for managing open ports and services. However, Reliability*First* also found that this documentation was insufficient as to its justification of why only the listed ports and services should be open. Therefore, Reliability*First* determined that URE had failed to fully address its violation of CIP-007-1 R2.

URE self-certified "Substantially Compliant" to CIP-007-1 R3. URE determined that its change management controls, as identified in its cyber security policy, only partially addressed this requirement because it does not allow for initial compliance or continued auditable compliance. URE's change management controls only espoused broad policies and did not explicitly describe the processes and programs to be established to manage changes. URE failed to establish, document, and implement a security patch management program in accordance with CIP-007-1 R3. URE also failed to assess security patches or upgrades for applicability within 30 calendar days of those patches' or upgrades' availability in accordance with CIP-007-1 R3.1 or document the implementation of security patches in accordance with CIP-007-1 R3.2. At the Unscheduled Audit, Reliability*First* discovered that URE's security patch management program allowed testing and installation of applicable security patches to be deferred. URE failed to provide for

[20] The Mitigation Plan incorrectly states that R5 and R6 each have a "Medium" VRF.

the implementation of compensating measures in the interim to mitigate risk exposure as required by CIP-007-1 R3.2.

On February 1, 2010, URE self-certified "Substantially Compliant" to CIP-007-1 R4. URE was "Substantially Compliant" because it determined that its malware prevention processes did not address this requirement by not allowing for initial compliance or continued auditable compliance. URE's malware prevention processes only espoused broad policies and did not explicitly describe the processes and programs to be established to prevent malware introduction, exposure, and propagation as required by CIP-007-1 R4. Additionally, URE failed to document and implement anti-virus and malware prevention tools on all servers and workstations. URE also failed to document and implement a process for updating anti-virus and malware prevention "signatures" in accordance with CIP-007-1 R4.2. At the Unscheduled Audit, Reliability*First* determined that URE had not completely addressed the violation of CIP-007-1 R4 by concluding that URE still had not documented and implemented a malware prevention policy. Specifically, Reliability*First* determined that URE failed to install anti-virus and malware software on certain of its printers and serial interface devices, in accordance with CIP-007-1 R4.

URE self-certified "Substantially Compliant" to CIP-007-1 R5. URE determined that its access control program did not adequately address this requirement. Specifically, URE: (i) failed to document technical and procedural controls to enforce access authentication of, and accountability for, all user activity in accordance with CIP-007-1 R5; (ii) failed to establish documented methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity in accordance with CIP-007-1 R5.1.2; and (iii) failed to require and use passwords subject to the criteria specified in CIP-007-1 R5.3. At the Unscheduled Audit, Reliability*First* further discovered that URE failed to document all generic accounts in accordance with CIP-007-1 R5.2.

URE self-certified "Substantially Compliant" to CIP-007-1 R6. URE determined that it failed to implement any automated tools or organizational process controls to monitor system events related to cyber security in accordance with CIP-007-1 R6. URE also failed to implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter in accordance with CIP-007-1 R6.1 and ensure that its security monitoring controls issued automated or manual alerts for detected Cyber Security Incidents in accordance with CIP-007-1 R6.2.

URE self-certified "Substantially Compliant" to CIP-007-1 R7. URE determined that it failed to document formal methods, processes, and procedures for disposal or redeployment of Cyber Assets. URE did not dispose of or redeploy any Cyber Assets within an Electronic Security Perimeter while it was non-compliant with CIP-007-1 R7.

URE self-certified "Substantially Compliant" to CIP-007-1 R9. URE determined that it lacked documentation of reviews and updates of the documentation specified in CIP-007-1. Additionally, URE failed to complete an annual review of all its documentation and failed to document changes resulting from modifications to the systems or controls within 30 calendar days of any change.

ReliabilityFirst determined the duration of the CIP-007-1 R1violation to be from July 1, 2008, the date on which URE was required to comply with CIP-007-1 R1 as a Table 1 entity for its System Control Center, through October 29, 2010, when URE completed its Mitigation Plan.

ReliabilityFirst determined the duration of the CIP-007-1 R2, R3, R4, R5, R6, R7, and R9 violations to be from July 1, 2009, the date on which URE was required to comply with CIP-007-1 R2, R3, R4, R5, R6, R7 and R9 as a Table 1 entity for its System Control Center, through October 29, 2010, when URE completed its Mitigation Plan.

CIP-008-1 R1

The purpose statement of CIP-008-1 provides in pertinent part: "Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."

CIP-008-1 R1 states in pertinent part:

> R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:
>
> > R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.
> >
> > R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.
> >
> > * * * * *
> >
> > R1.4. Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.
> >
> > R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
> >
> > R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

CIP-008-1 R1 has a "Lower" VRF.

At the Spot Check, ReliabilityFirst discovered that URE failed to maintain procedures to characterize and classify events as reportable Cyber Security Incidents in violation of CIP-008-1 R1. ReliabilityFirst reviewed two versions of URE's Cyber Security Policy because both were effective during the time period covered by the Spot Check. Both versions contained minimal reporting procedures for cyber security incidents, and neither version contained procedures to

characterize and classify events as reportable Cyber Security Incidents in accordance with CIP-008-1 R1.1. Reliability*First* also determined that both versions failed to address the following: (i) Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and internal communication plans in accordance with CIP-008-1 R1.2; (ii) a process for updating the Cyber Security Incident response plan within ninety calendar days of any changes in accordance with CIP-008-1 R1.4; (iii) a process for ensuring that the Cyber Security Incident response plan is reviewed at least annually in accordance with CIP-008-1 R1.5; and (iv) a process for ensuring the Cyber Security Incident response plan is tested at least annually in accordance with CIP-008-1 R1.6.

Reliability*First* determined the duration of the violation to be from July 1, 2008, the date on which URE was required to comply with CIP-008-1 R1 as a Table 1 entity for its System Control Center, through April 12, 2010, when URE completed its Mitigation Plan.

CIP-009-1 R1, R3 and R4

The purpose statement of CIP-009-1 provides in pertinent part: "Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."

CIP-009-1 states in pertinent part:

> R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets.
>
> * * * * *
>
> R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change
>
> R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

CIP-009-1 R1 has a "Medium" VRF while R3 and R4 have a "Lower" VRF.

At the Spot Check, Reliability*First* discovered a violation of CIP-009-1 R1 by concluding that URE failed to specify the actions that would be required to respond to events or conditions of varying duration and severity that would activate its Critical Cyber Asset recovery plan. Reliability*First* reviewed the portions of URE's Cyber Security Policy addressing URE's recovery plans for Critical Cyber Assets. The Cyber Security Plan stated generally that URE would switch to its fully redundant backup control center in the event that a cyber security incident resulted in the loss of Critical Cyber Assets at the primary control center. This policy

did not specify the required actions URE must take in order to recover the lost Critical Cyber Assets.

URE self-certified "Substantially Compliant" to CIP-009-1 R3. URE failed to update its recovery plan to reflect changes or lessons learned from exercises or actual incidents by failing to note that the exercises performed on URE's previous recovery plan demonstrated no necessary changes or lessons learned.

URE self-certified "Substantially Compliant" to CIP-009-1 R4. URE determined that it failed to include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets in the recovery plan provisions of its Cyber Security Policy. URE, however, represents that it did backup and store information required to successfully restore its Critical Cyber Assets, despite its failure to document these activities in its recovery plan.

Reliability*First* determined the duration of the CIP-009-1 R1 violation to be from July 1, 2008, the date on which URE was required to comply with CIP-009-1 R1 as a Table 1 entity for its System Control Center, through June 2, 2010, when URE completed its Mitigation Plan.

Reliability*First* determined the duration of the CIP-009-1 R3 and R4 violation to be from July 1, 2009, the date on which URE was required to comply with CIP-009-1 R3 and R4 as a Table 1 entity for its System Control Center, through June 2, 2010, when URE completed its Mitigation Plan.

Reliability Impact Statement – Potential and Actual

Reliability*First* determined that these violations, taken individually, do not pose a serious or substantial risk to the reliability of the bulk power system (BPS). In the aggregate, however, there was potential for substantial risk to the reliability of the BPS because failure to document the full range of protections afforded in CIP-002-1 through CIP-009-1 and the processes and procedures through which these protections are maintained compromised integrity of its identified Critical Cyber Assets. URE mitigated this risk by implementing mitigation plans and promptly implementing a revised CIP compliance program. URE's cyber security policy in place at the time of the Spot Check evidenced URE's awareness of the importance of maintaining cyber security. Additionally, URE took actions to protect Critical Cyber Assets, such as denying access to those assets by default and implementing firewalls to protect its Electronic Security Perimeter. URE has also committed to future implementation of measures that will enhance the reliability of the bulk electric system beyond that which is required by the Reliability Standards. All of these risk considerations have been taken into consideration.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, Reliability*First* has assessed a penalty of seventy thousand dollars ($70,000) for the referenced violations. In reaching this determination, Reliability*First* considered the following factors:

(1) Additional, non-related violations of the following NERC Reliability Standards were either self reported or discovered during a compliance audit: PRC-005-1 R2.1; CIP-001-1 R1; EOP-

001-0 R3, R4, R5, and R6; FAC-003-1 R1 and R2; FAC-008-1 R1; and VAR-001-1 R1. These additional violations were resolved in a separate Settlement Agreement executed November 22, 2010. Reliability*First* and URE negotiated Settlement Agreements resolving both the above violations and those discussed herein simultaneously. Reliability*First* considered the commitments and actions set forth in both Agreements when determining the final monetary penalty set forth in each Agreement.

(2) URE has an Internal Compliance Program (ICP) which seeks to ensure compliance with all applicable NERC Reliability Standards.

(3) URE has agreed to take actions that exceed those actions that would be expected to achieve and maintain baseline compliance. These actions enhance the reliability of the BPS beyond baseline compliance and are viewed favorably in conjunction with the overall level of penalty and other terms and conditions of the Settlement Agreement. Descriptions of these above and beyond actions are set forth in the Settlement Agreement.

After consideration of the above factors, Reliability*First* determined that, in this instance, the penalty amount of seventy thousand dollars ($70,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[21]

CIP-002-1 R1
URE's Mitigation Plan to address its violation of CIP-002-1 R1 was submitted to Reliability*First* on September 3, 2010 with a proposed completion date of April 12, 2010. The Mitigation Plan was accepted by Reliability*First* on September 13, 2010[22] and approved by NERC on October 7, 2010. The Mitigation Plan for this violation is designated as MIT-08-2849 and was submitted as non-public information to FERC on October 7, 2010.

URE's Mitigation Plan required URE to ensure that its Cyber Security Policy contained sufficient detail to maintain compliance with CIP-002 through CIP-009. URE noted that it initially corrected the violation by making its Cyber Security Policy effective on July 15, 2008.[23] In subsequently reviewing its Cyber Security Policy, however, URE recognized a need to revise this policy further. URE developed a number of documents to do so.

URE certified on October 29, 2010 that the above Mitigation Plan requirements were completed on April 12, 2010. As evidence of completion of its Mitigation Plan, URE submitted documents created to address the violation of CIP-002-1 which are listed in the Mitigation Plan.

On April 16, 2010, after reviewing URE's submitted evidence at the Unscheduled Audit, Reliability*First* verified that URE's Mitigation Plan was completed on April 12, 2010.

[21] *See* 18 C.F.R § 39.7(d)(7).
[22] The Settlement Agreement incorrectly states that the Mitigation Plan was accepted by Reliability*First* was accepted on September 10, 2010.
[23] The Settlement Agreement incorrectly states that the effective date of the Cyber Security Policy.

CIP-003-1 R1, R4, R5 and R6

URE's Mitigation Plan to address its violations of CIP-003-1 R1, R4, R5 and R6 was submitted to Reliability*First* on September 3, 2010 with a proposed completion date of October 31, 2010. The Mitigation Plan was accepted by Reliability*First* on September 13, 2010 and approved by NERC on October 7, 2010. The Mitigation Plan for this violation is designated as MIT-08-2850 and was submitted as non-public information to FERC on October 7, 2010.

URE's Mitigation Plan required URE to create new policies and procedures to ensure that all the requirements of the CIP Reliability Standards are addressed, that information is protected, that the list of personnel with access to protected information is documented, and that changes to URE's policies and procedures are managed.

URE certified on October 29, 2010 that the above Mitigation Plan requirements were completed on October 29, 2010. As evidence of completion of its Mitigation Plan, URE submitted documents created to address the violations of CIP-003-1 which are listed in the Mitigation Plan and Verification of Mitigation Plan Completion.

On March 29, 2011, after reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed on October 29, 2010.

CIP-004-1 R2, R3 and R4

URE's Mitigation Plan to address its violations of CIP-004-1 R2, R3 and R4 was submitted to Reliability*First* on September 7, 2010[24] with a proposed completion date of April 12, 2010. The Mitigation Plan was accepted by Reliability*First* on September 13, 2010 and approved by NERC on October 7, 2010. The Mitigation Plan for this violation is designated as MIT-08-2851 and was submitted as non-public information to FERC on October 7, 2010.

URE's Mitigation Plan required URE to train the relevant personnel and conducted personnel risk assessments on the relevant personnel. To correct URE's access lists and ensure that similar violations do not occur in the future, URE created new policies and procedures.

URE certified on October 29, 2010 that the above Mitigation Plan requirements were completed on April 12, 2010. As evidence of completion of its Mitigation Plan, URE submitted documents created to address the violations of CIP-004-1 which are listed in the Mitigation Plan.

On April 16, 2010, after reviewing URE's submitted evidence at the Unscheduled Audit, Reliability*First* verified that URE's Mitigation Plan was completed on April 12, 2010.

CIP-005-1 R1, R2, R3 and R5[25]

URE's Mitigation Plan to address its violations of CIP-005-1 R1, R2, R3 and R5 was submitted to Reliability*First* on September 3, 2010 with a proposed completion date of October 31, 2010.

[24] The Mitigation Plan is dated September 3, 2010.
[25] The Mitigation Plan for the CIP-005 violations also references a violation of CIP-005-1 R4. Reliability*First* dismissed this alleged violation on November 11, 2010.

The Mitigation Plan was accepted by Reliability*First* on September 13, 2010 and approved by NERC on October 7, 2010. The Mitigation Plan for this violation is designated as MIT-10-2855 and was submitted as non-public information to FERC on October 7, 2010.

URE's Mitigation Plan required URE to update its Electronic Security Perimeter drawings to accurately reflect all access points to the Electronic Security Perimeter. URE also committed to revise is policies and procedures to ensure that its Electronic Security Perimeter is protected and controlled in accordance with CIP-005-1.

URE certified on October 29, 2010 that the above Mitigation Plan requirements were completed on October 29, 2010. As evidence of completion of its Mitigation Plan, URE submitted documents created to address the violations of CIP-005-1which are listed in the Mitigation Plan and Verification of Mitigation Plan Completion.

On April 22, 2011, after reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed on October 29, 2010 and that URE was in compliance with CIP-005-1.

CIP-006-1 R1 and R3

URE's Mitigation Plan to address its violations of CIP-006-1 R1 and R3 was submitted to Reliability*First* on September 3, 2010 with a proposed completion date of April 12, 2010. The Mitigation Plan was accepted by Reliability*First* on September 13, 2010 and approved by NERC on October 7, 2010. The Mitigation Plan for this violation is designated as MIT-10-2856 and was submitted as non-public information to FERC on October 7, 2010.

URE's Mitigation Plan required URE to revise its policies and procedures to ensure that all access points to Physical Security Perimeters are identified and that these access points are monitored and controlled as required by CIP-006-1.

URE certified on October 29, 2010 that the above Mitigation Plan requirements were completed on April 12, 2010. As evidence of completion of its Mitigation Plan, URE submitted documents created to address the violations of CIP-006-1which are listed in the Mitigation Plan.

On April 16, 2010, after reviewing URE's submitted evidence at the Compliance Audit, Reliability*First* verified that URE's Mitigation Plan was completed on April 12, 2010 and that URE was in compliance with CIP-006-1.

CIP-007-1 R1, R2, R3, R4, R5, R6, R7 and R9

URE's Mitigation Plan to address its violations of CIP-007-1 R1, R2, R3, R4, R5, R6, R7 and R9 was submitted to Reliability*First* on September 3, 2010 with a proposed completion date of October 31, 2010. The Mitigation Plan was accepted by Reliability*First* on September 13, 2010 and approved by NERC on October 7, 2010. The Mitigation Plan for this violation is designated as MIT-08-2852 and was submitted as non-public information to FERC on October 7, 2010.

URE's Mitigation Plan required URE to revise its policies and procedures to ensure that these policies and procedures address all the requirements of CIP-007-1.

URE certified on October 29, 2010 that the above Mitigation Plan requirements were completed on October 29, 2010. As evidence of completion of its Mitigation Plan, URE submitted documents created to address the violations of CIP-007-1which are listed in the Mitigation Plan.

On May 3, 2011, after reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed on October 29, 2010 and that URE was in compliance with CIP-007-1.

CIP-008-1 R1[26]
URE's Mitigation Plan to address its violation of CIP-008-1 R1 was submitted to Reliability*First* on September 3, 2010 with a proposed completion date of April 12, 2010. The Mitigation Plan was accepted by Reliability*First* on September 13, 2010 and approved by NERC on October 7, 2010. The Mitigation Plan for this violation is designated as MIT-08-2853 and was submitted as non-public information to FERC on October 7, 2010.

URE's Mitigation Plan required URE to revise its policies and procedures to ensure that they address the deficiencies with CIP-008-1.

URE certified on October 29, 2010 that the above Mitigation Plan requirements were completed on April 12, 2010. As evidence of completion of its Mitigation Plan, URE submitted documents created to address the violation of CIP-008-1.

On April 16, 2010, after reviewing URE's submitted evidence at the Compliance Audit, Reliability*First* verified that URE's Mitigation Plan was completed on April 12, 2010 and that URE was in compliance with CIP-008-1.

CIP-009-1 R1, R3 and R4[27]
URE's Mitigation Plan to address its violation of CIP-009-1 was submitted to Reliability*First* on September 3, 2010 with a proposed completion date of June 2, 2010.[28] The Mitigation Plan was accepted by Reliability*First* on September 13, 2010 and approved by NERC on October 7, 2010. The Mitigation Plan for this violation is designated as MIT-08-2854 and was submitted as non-public information to FERC on October 7, 2010.

URE's Mitigation Plan required URE to revise its policies and procedures to address these deficiencies.

URE certified on October 29, 2010 that the above Mitigation Plan requirements were completed on June 2, 2010. As evidence of completion of its Mitigation Plan, URE documents created to address the violations of CIP-009-1 R1, R3, and R4 which are listed in the Mitigation Plan.

[26] The Mitigation Plan for the CIP-008 violation also references a violation of CIP-008-1 R2. Reliability*First* dismissed this alleged violation on November 11, 2010.
[27] The Mitigation Plan for the CIP-009 violations also references a violation of CIP-009-1 R2 and R5. Reliability*First* dismissed these alleged violations on November 11, 2010.
[28] Section D.2 of the Mitigation Plan incorrectly states that the Mitigation Plan was completed on April 12, 2010.

On April 25, 2011, after reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed on June 2, 2010 and that URE was in compliance with CIP-009-1.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[29]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[30] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on February 15, 2011. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of a seventy thousand dollar ($70,000) 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 violations of the subject NERC Reliability Standards;
2. Reliability*First* reported that URE was cooperative throughout the compliance enforcement process;
3. URE had a compliance program at the time of the violation which Reliability*First* 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. URE has agreed to take actions that exceed those actions that would be expected to achieve and maintain baseline compliance, which Reliability*First* considered a mitigating factor, as discussed in the Settlement Agreement; and
6. Reliability*First* reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and assessed penalty of seventy thousand dollars ($70,000) as appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[29] *See* 18 C.F.R. § 39.7(d)(4).

[30] *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 Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Request for Confidential Treatment

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

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

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

Attachments to be Included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between Reliability*First* and URE executed November 22, 2010, included as Attachment a;

    a. URE's Summary for Possible Violation for CIP-002-1 R1, included as Attachment A;

    b. URE's Summary for Possible Violation for CIP-003-1 R1, included as Attachment B;

    c. URE's Summary for Possible Violation for CIP-004-1 R2, included as Attachment C;

    d. URE's Summary for Possible Violation for CIP-004-1 R3, included as Attachment D;

    e. URE's Summary for Possible Violation for CIP-004-1 R4, included as Attachment E;

    f. URE's Summary for Possible Violation for CIP-007-1 R1, included as Attachment F;

    g. URE's Summary for Possible Violation for CIP-008-1 R1, included as Attachment G;

    h. URE's Summary for Possible Violation for CIP-009-1 R1, included as Attachment H;

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

i. Self Certification for CIP-003-1 R4, R5 and R6; CIP-005-1 R1, R2, R3 and R5; CIP-006-1 R1 and R3; CIP-007-1 R2, R3, R4, R5, R6, R7 and R9; and CIP-009-1 R3 and R4, included as Attachment I;

j. URE's Mitigation Plan designated as MIT-08-2849 for CIP-002-1 R1, included as Attachment J;

k. URE's Certification of Mitigation Plan Completion for CIP-002-1 R1, included as Attachment K;

l. URE's Mitigation Plan designated as MIT-08-2850 for CIP-003-1 R1, R4, R5 and R6, included as Attachment L;

m. URE's Certification of Mitigation Plan Completion for CIP-003-1 R1, R4, R5 and R6, included as Attachment M;

n. URE's Mitigation Plan designated as MIT-08-2851 for CIP-004-1 R2, R3 and R4, included as Attachment N;

o. URE's Certification of Mitigation Plan Completion for CIP-004-1 R2, R3 and R4, included as Attachment O;

p. URE's Mitigation Plan designated as MIT-10-2855 for CIP-005-1 R1, R2, R3 and R5, included as Attachment P;

q. URE's Certification of Mitigation Plan Completion for CIP-005-1 R1, R2, R3 and R5, included as Attachment Q;

r. URE's Mitigation Plan designated as MIT-10-2856 for CIP-006-1 R1 and R3, included as Attachment R;

s. URE's Certification of Mitigation Plan Completion for CIP-006-1 R1 and R3, included as Attachment S;

t. URE's Mitigation Plan designated as MIT-08-2852 for CIP-007-1 R1, R2, R3, R4, R5, R6, R7 and R9, included as Attachment T;

u. URE's Certification of Mitigation Plan Completion for CIP-007-1 R1, R2, R3, R4, R5, R6, R7 and R9, included as Attachment U;

v. URE's Mitigation Plan designated as MIT-08-2853 for CIP-008-1 R1, included as Attachment V;

w. URE's Certification of Mitigation Plan Completion for CIP-008-1 R1, included as Attachment W;

x. URE's Mitigation Plan designated as MIT-08-2854 for CIP-009-1 R1, R3 and R4, included as Attachment X;

y. URE's Certification of Mitigation Plan Completion for CIP-009-1 R1, R3 and R4, included as Attachment Y;

b) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-002-1 R1, included as Attachment b;

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

c) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-003-1 R1, R4, R5 and R6, included as Attachment c;

d) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-004-1 R2, R3 and R4, included as Attachment d;

e) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-005-1 R1, R2, R3 and R5, included as Attachment e;

f) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-006-1 R1 and R3 , included as Attachment f;

g) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-007-1 R1, R2, R3, R4, R5, R6, R7 and R9, included as Attachment g;

h) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-008-1 R1, included as Attachment h; and

i) Reliability*First*'s Verification of Mitigation Plan Completion for CIP-009-1 R1, R3 and R4, included as Attachment i.

A Form of Notice Suitable for Publication[31]

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

[31] *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	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Davis Smith* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net davis.smith@nerc.net Robert K. Wargo* Director of Enforcement and Regulatory Affairs Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 bob.wargo@rfirst.org L. Jason Blake* Managing Enforcement Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 jason.blake@rfirst.org Michael D. Austin* Associate Attorney 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 mike.austin@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ *Rebecca J. Michael*

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Sr. Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Davis Smith
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
davis.smith@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

Attachments