PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

April 30, 2012

Ms. Kimberly D. 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. NP12-_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, 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]

URE submitted to Reliability*First* Corporation (Reliability*First*) self reports of possible violations of nine CIP Standards listed as follows: CIP-007-1 R3, CIP-007-3 R4.1, CIP-007-3 R6, CIP-004-2 R4.2, CIP-002-3 R3, CIP-006-3 R1, CIP-007-3 R1, CIP-007-3 R2, and CIP-007-3 R6.

Reliability*First* conducted a Compliance Audit of URE, during which Reliability*First* discovered eight additional CIP violations of the following Standards: CIP-005-3 R1.4, CIP-005-3 R 2.2, CIP-005-3 R3.2, CIP-005-3 R4.2, CIP-007-3 R2.1, CIP-007-3 R3, CIP-007-3 R5, and CIP-007-3 R8.2.

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

[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 (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).

[2] *See* 18 C.F.R § 39.7(c)(2).

determination and findings of the violations[3] of the standards described above. According to the Settlement Agreement, URE agrees and stipulates to the facts in the Agreement, but has agreed to the assessed penalty of one hundred and fifteen thousand dollars ($115,000), 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 RFC201000452, RFC201000453, RFC201000454, RFC201000460, RFC201100733, RFC201100734, RFC201100735, RFC201100736, RFC201100737, RFC201100760, RFC201100761, RFC201100762, RFC201100763, RFC201100764, RFC201100765, RFC201100766, and RFC201100767 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 executed on August 26, 2011, 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 ($) |
|---|---|---|---|---|---|---|---|
| | | | RFC201000452 | CIP-007-1 | 3.1; 3.2 | Lower | |
| | | | RFC201000453 | CIP-007-3 | 4.1[4] | Medium | |

[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 or confirmed violation.

[4] 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.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| RFC | Unidentified Registered Entity | NCRXXXXX | RFC201000454 | CIP-007-3 | 6 | Lower | 115,000 |
| | | | RFC201000460 | CIP-004-2 | 4.2[5] | Medium | |
| | | | RFC201100733 | CIP-002-3 | 3.2 | Lower | |
| | | | RFC201100734 | CIP-006-3 | 1.1 | Medium | |
| | | | RFC201100735 | CIP-007-3 | 1.1 | Medium | |
| | | | RFC201100736 | CIP-007-3 | 2 | Medium | |
| | | | RFC201100737 | CIP-007-3 | 6.1; 6.5 | Lower | |
| | | | RFC201100760 | CIP-005-3 | 1.4 | Medium | |
| | | | RFC201100761 | CIP-005-3 | 2.2 | Medium | |
| | | | RFC201100762 | CIP-005-3 | 3.2 | Medium | |
| | | | RFC201100763 | CIP-005-3 | 4.2 | Medium | |
| | | | RFC201100764 | CIP-007-3 | 2.1 | Medium | |
| | | | RFC201100765 | CIP-007-3 | 3.1;3.2 | Lower | |
| | | | RFC201100766 | CIP-007-3 | 5.1.2; 5.1.3; 5.3.2 | Lower[6]/ Medium | |
| | | | RFC201100767 | CIP-007-3 | 8.2 | Medium | |

[5]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.

[6]URE's violation of CIP-007-3 R5 implicated R5.1.2, which has a VRF of "Lower," R5.1.3, which has a VRF of "Medium," and R5.3.2, which has a VRF of "Lower."

**SELF-REPORTED VIOLATIONS**

**CIP-007-1 R3.1 and R3.2 (RFC201000452)**

The purpose of Reliability Standard CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities[7] 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 R3 provides:

> **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.

CIP-007-1 R3 has a "Lower" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE submitted a Self-Report to Reliability*First*. URE stated that it had in place a documented security patch management program. Nevertheless, during an internal audit, URE discovered that it failed to include a provision requiring personnel to document the assessment and implementation of security patches in that program for certain Cyber Assets.

[7] Within the text of Standard CIP-002 – CIP-009, "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.

Reliability*First* determined that URE's failure to document the assessment and implementation of security patches resulted from its failure to implement a comprehensive method for doing so across all business units. Specifically, URE failed to successfully identify the personnel responsible for these tasks for cyber assets owned or managed by multiple business units. In addition, URE incorrectly configured its reporting tool, which resulted in vulnerability assessments that did not include all cyber assets within every Electronic Security Perimeter (ESP). URE failed to regularly conduct vulnerability scans because personnel lacked a clear understanding of the capabilities of its reporting tool.

Reliability*First* determined that URE failed to document the assessment of security patches and security upgrades within thirty calendar days of availability of the patches or upgrades in violation of CIP-007-1 R3.1, and failed to document the implementation of security patches, in violation of R3.2.

Reliability*First* determined the duration of the violation is from the date URE was required to comply with this Standard, to the date URE completed its Mitigation Plan.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because all assets at issue were located in a secured Physical Security Perimeter (PSP) to which a limited number of individuals had access. The individuals with access had NERC cyber security training and a valid Personnel Risk Assessment (PRA). All assets in question resided on isolated networks with no direct access to the corporate network or the Internet, and all traffic to and from said networks traversed secured access points. Finally, although URE did not maintain documentation for the evaluation process to determine the applicability of patches or where patches were not installed due to non-applicability, URE maintained documentation of patch installation for those Cyber Assets to which it applied patches as part of its established configuration management process.

**Status of Mitigation Plan**[8]

URE's Mitigation Plan to address its violations of CIP-007-1 R3.1 and R3.2 was submitted to Reliability*First* on October 18, 2010 with a proposed completion date of November 19, 2010. The Mitigation Plan was accepted by Reliability*First* on November 16, 2010 and approved by NERC on December 7, 2010. The Mitigation Plan for these violations is designated as MIT-10-3094[9] and was submitted as non-public information to FERC on December 10, 2011 in accordance with FERC orders.

[8] *See* 18 C.F.R § 39.7(d)(7).
[9] This Mitigation Plan addressed the following CIP violations: RFC201000452, RFC201000453 and RFC201000454.

According to the Mitigation Plan, URE:

1. Revised its governing documents to provide direct guidance on the documentation required for the assessment and implementation of security patches and security upgrades. This revision involved process testing and training of personnel, as well as tests to require post-installation validation of all patch installation;

2. Developed a single, comprehensive process to ensure that the configuration of its reporting tool produces consistent, comprehensive reports; and

3. Reinforced its change control process by revising its governing change control documents to provide prescriptive direction regarding the required documentation changes.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Vulnerability management assessment program; and
2. A plant order regarding the change management process for CIP assets.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-007-1 R3.

**CIP-007-3 R4.1 (RFC201000453)**

The purpose of Reliability Standard CIP-007-3 provides: "Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered CIP-002-3 through CIP-009-3."

CIP-007-3 R4.1 provides in pertinent part:

> **R4.** Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
>
> > **R4.1.**The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware

prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

CIP-007-3 R4.1 has a "Medium" VRF and a "Severe" VSL. T

URE submitted a Self-Report to Reliability*First* stating that during its internal audit, URE discovered that it failed to document certain anti-virus and malware prevention tools. URE failed to document and implement anti-virus protection for nine of its Critical Cyber Assets (CCAs) and Cyber Assets within one of its ESPs at one of its facilities. The implicated assets constitute 2.63% of URE's Cyber Assets within an ESP, including CCAs. The anti-virus tools for these nine devices were in various states of implementation. Some of the devices' anti-virus engines were not functioning properly, some of the devices' anti-virus engines were not reporting to the central console, and some of the devices were not technically capable of running malware tools.

In addition, URE discovered that it failed to install anti-virus software on three Cyber Assets within an ESP in the Systems Operations Center (SOC). During the internal audit, URE discovered that the vendor responsible for implementing malware tools installed Cyber Assets without following procedures to ensure malware was properly installed prior to placing these Cyber Assets into production. Therefore, URE failed to implement anti-virus and malware protection tools for certain Cyber Assets within this ESP. These discrepancies resulted from a deficiency in URE's implementation of its software that manages and reports on the status of anti-virus and malware protection for Cyber Assets within the ESP, including CCAs. URE's process lacked an embedded test to verify that all Cyber Assets in the ESP are included in its report on the status of anti-virus and malware protection.

URE also discovered that one CCA within the ESP was not technically capable of running the anti-virus and anti-malware software, but URE failed to submit a Technical Feasibility Exception (TFE) for this CCA prior to its recognition of the issue underlying this violation.

As a result, Reliability*First* determined that URE violated CIP-007-3 R4.1 for failure to document and implement anti-virus and malware prevention tools for all Cyber Assets within the ESP.

Reliability*First* determined the duration of the violation to be from the date URE was required to comply with this Standard, to the date URE completed its Mitigation Plan.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because the risk was mitigated by the fact that URE implemented all required anti-virus software, except as identified above. In addition, all assets at issue were located in a secured PSP to which a limited number of individuals had access. All of those with

access to the PSP had NERC cyber security training and a valid PRA. All assets in question resided on isolated networks with no direct access to the corporate network or the internet, and all traffic to and from said networks traversed secured access points.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-007-3 R4.1 was submitted to Reliability*First* on October 18, 2010 with a proposed completion date of November 19, 2010. The Mitigation Plan was accepted by Reliability*First* on November 16, 2010 and approved by NERC on December 7, 2010. The Mitigation Plan for this violation is designated as MIT-10-3094 and was submitted as non-public information to FERC on December 10, 2010 in accordance with FERC orders.

According to the Mitigation Plan, URE:

1. Developed and implemented a process to ensure that the anti-virus monitoring report is validated against the list of Cyber Assets within the ESP;

2. Reviewed and revised its internal review process for vendor-supplied Cyber Assets within the ESP; and

3. Submitted TFE requests regarding the CCA within the ESP that was not technically capable of running the anti-virus and anti-malware software.

URE certified that the Mitigation Plan was completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. A program that requires cross-referencing the antivirus management console's report against the lists of protected Cyber Assets;
2. A list of Cyber Assets which require anti-virus protection and a list of those assets configured for ant-virus for several facilities; and
3. The revised Technical Feasibility Exception requests.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-007-3 R4.1.

**CIP-007-3 R6 (RFC201000454)**

CIP-007-3 R6 provides in pertinent part: **"**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."

CIP-007-3 R6 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that during its internal audit, URE discovered that it failed to implement automated tools or organizational process controls to monitor system events related to cyber security for ten Cyber Assets within the ESP. Specifically, for ten Cyber Assets within its ESPs, URE's network configuration utilized both domain account logon and local account logon, which allowed local, authenticated access in the event of a domain or network failure. However, the failed local logon attempts were not aggregated and communicated to the domain controller. Therefore, URE failed to monitor those logon attempts, which are system events related to cyber security.

In addition, URE failed to configure the domain monitoring system for security monitoring for these ten Cyber Assets within the ESP.

Reliability*First* determined that URE violated CIP-007-3 R6 for failure to ensure that all Cyber Assets within the ESP implement automated tools or organizational process controls to monitor system events that are related to cyber security.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because the risk was mitigated by the fact that URE had enabled local logging on the local device to track and retain logs of authenticated and unauthenticated events. All assets in question resided on isolated networks with no direct access to the corporate network or the internet, and all traffic to and from said networks traversed secured access points. Furthermore, all assets at issue were located in a secured PSP to which a very limited number of individuals had access. All of those with access to the PSP had NERC cyber security training and a valid PRA.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-007-3 R6 was submitted to Reliability*First* on October 18, 2010 with a proposed completion date of November 19, 2010. The Mitigation Plan was

accepted by Reliability*First* on November 16, 2010 and approved by NERC on December 7, 2010. The Mitigation Plan for this violation is designated as MIT-10-3094 and was submitted as non-public information to FERC on December 10, 2010 in accordance with FERC orders.

According to the Mitigation Plan, URE:

1. Installed the domain monitoring system on all Cyber Assets that did not have it;

2. Identified and configured security status monitoring on the Cyber Assets within the ESP that did not have it; and

3. Reviewed and corrected the configuration of all assets that are technically capable of being monitored within all ESPs.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. The NERC CIP Cyber Assets for specific facilities;
2. Screenshot from each Power Plant's monitoring client;
3. Validation of the routers;
4. Validation of the switches;
5. Screenshots of the configuration file for each Router and Switch in the Power plant environment;
6. Screenshots of the configuration of the monitoring client for the systems in the ESP at each Power Plant location;
7. The WINEVENT Alias file for each site demonstrating from which devices the monitoring client is collecting data;
8. Screenshots of the firewall configuration at each plant location;
9. The list of all the Critical Cyber Assets in the SOC;
10. Documents that demonstrate the consoles and Windows Servers that are monitored by a Windows Event Interface;
11. Documents that demonstrate the machines that are not monitored by a Windows Event Interface;
12. Screenshots of each device's configuration to send a notification to the subject matter expert's e-mail;
13. Documents that demonstrate that the routers are logging and monitoring Failed Attempts and Passed Authentications; and
14. Screenshots of the configuration field for each Router in the SOC.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-007-3 R6.

**CIP-004-2 R4.2 (RFC201000460)**

The purpose of Reliability Standard CIP-004-2 provides: "Standard CIP-004-2 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-004-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2."

CIP-004-2 R4.2 provides in pertinent part:

> **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.
>
> > **R4.2.** 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-004-2 R4.2 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First*, stating that it had identified two instances where it failed to timely revoke an individual's access to CCAs. URE's contract security company terminated a contract security officer(not for cause). This security officer had authorized unescorted physical access to CCAs. A month and a half later, URE discovered during a routine review that it failed to revoke the security officer's authorized unescorted physical access rights, and then promptly revoked such access. Therefore, URE failed to revoke the individual's access within the required seven days, in violation of this Standard.

URE's contract security company terminated another contract security officer for cause, which was unrelated to the CIP Standards, and confiscated his access badge. This security officer had authorized unescorted physical access to CCAs. Two days after the termination, URE discovered that it failed to revoke the individual's authorized unescorted physical access rights, and then promptly revoked the individual's access. Therefore, URE failed to revoke the individual's access within the required 24 hours in violation of this Standard.

Reliability*First* determined that the duration of the violation for the first incident was seven days after URE's contract security company terminated the security officer not for cause, to the date URE revoked his access.

Reliability*First* determined that the duration of this violation for the second incident was from J24 hours after URE's contract security company terminated the Security officer for cause, to the date URE revoked his access.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because the security officer who was terminated for cause did not have his access badge during the time period of the violation, because URE confiscated his access badge upon his termination. As a result, this security officer could not have physically accessed URE's CIP areas. In addition, neither of the two security officers in question physically accessed any areas containing CCAs after their terminations.

**Status of Mitigation Plan**

Reliability*First*'s Mitigation Plan to address its violation of CIP-004-2 R4.2 was submitted to Reliability*First* on September 3, 2010 with a proposed completion date of October 15, 2010.[10] The Mitigation Plan was accepted by Reliability*First* September 15, 2010 and approved by NERC on October 7, 2010. The Mitigation Plan for this violation is designated as MIT-10-2859 and was submitted as non-public information to FERC on October 7, 2010 in accordance with FERC orders.

According to the Mitigation Plan, URE:

1. Informed the contract security company of the incidents, and:

    a. After the first incident, URE provided training to the contract security company on the requirements of CIP-004 R4.2;

    b. After the second incident, URE advised the contract security company that a contract security account manager was responsible for the incident;

2. Required all contract security account managers to review applicable CIP procedures. Subsequently, the contract security company developed an internal procedure governing the removal of access rights;

[10] The Mitigation Plan for the CIP-004-2 R4.2 violation was signed on July 21, 2010.

3. Implemented procedures to assist with the tracking of contractors;

4. Conducted a spot audit of the contract security company's PRAs and found no anomalies;

5. Revised its procedures so that all individuals with physical access rights to CCA areas must have the access badge on their person in order to enter the area. URE no longer permits access privileges for those individuals who do not have the badge on their person; and

6. Required all supervisors of contractors with physical access rights to CCA areas to review CIP-004 requirements, to sign off that they did so, and to receive quarterly informational updates regarding CIP-004 and applicable security procedures.

URE certified that this Mitigation Plan was completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. A document showing the signatures and dates of participants stating that they have re-reviewed URE's CIP security procedures;
2. A procedure on background screening and CIP training verification, and processing/revocation of unescorted physical access privileges;
3. a list of names of contractors that URE required to be added to their database;
4. A document that identifies what happed to cause the alleged violation, lessons learned as a result of the alleged violation and a list of actions/decisions to be made to address the causes;
5. A document on Physical Access requirements; and
6. Copies of attestations signed by participants affirming that the participant has read the NERC Physical Access documents.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-004-2 R4.2.

**CIP-002-3 R3.2 (RFC211000733)**

The purpose of Reliability Standard CIP-002-3 provides in pertinent part:

> NERC Standards CIP-002-3 through CIP-009-3 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-002-3 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-002-3 R3 provides in pertinent part:

> 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 at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time 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-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> R3.2. The Cyber Asset uses a routable protocol within a control center.

CIP-002-3 R3.2 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First*, stating that it had conducted an internal audit at which it discovered that it failed to include certain assets on its CCA list. Specifically, URE failed to include 85 Cyber Assets that use a routable protocol within a control center on its list of Critical Cyber Assets essential to the operation of Critical Assets. These Cyber Assets are located in various locations.

Based on the Self-Report, Reliability*First* determined that URE violated CIP-002-3 R3.2 for failure to include all required Cyber Assets in its list of associated CCAs essential to the operation of the Critical Asset.

Reliability*First* determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE updated its CCA list.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a minimal risk to the reliability of the BPS because although URE submitted an incomplete list of CCAs to Reliability*First*, URE separately maintained a list of CCAs that was broader than the list initially approved by senior management and submitted to Reliability*First*. URE relied upon the broader, separately-maintained list of CCAs at all relevant times, which included all required assets within the ESPs. URE therefore provided CCA protections to the full list of CCAs, despite having the incorrect list approved by the senior management.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-002-3 R3.2 was submitted to Reliability*First* on April 18, 2011 with a proposed completion date of November 24, 2010. The Mitigation Plan was accepted by Reliability*First* on May 5, 2011, and approved by NERC on June 9, 2011. The Mitigation Plan for this violation is designated as MIT-10-3658 and was submitted as non-public information to FERC on June 9, 2011 in accordance with FERC orders.

According to the Mitigation Plan, URE revised its lists of CCAs, Cyber Assets, and non-critical Cyber Assets within the ESP to reflect the production environment.

URE submitted a certification of completion for this Mitigation Plan to Reliability*First*, which stated that URE completed this Mitigation Plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. A document describing the Mitigation Plan to correct the CCA list deficiencies identified by an internal audit;
2. A summary of the original and revised CCA list of bookmarks signed by a CIP manager; and
3. A list of the original and revised CCA lists referenced in the above document.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-002-3 R3.2.[11]

**CIP-006-3 R1.1 (RFC201100734)**

The purpose of Reliability Standard CIP-006-3 provides: "Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-006-3 R1 provides in pertinent part:

> **R1.** Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

[11] The Standard in the Verification of Mitigation Plan Completion is listed as CIP-002-1 R3.

> **R1.1.** All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (six-wall) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

CIP-006-3 R1.1 has a "Medium" and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that during the internal audit, URE discovered that its network configuration utilized an alternate method of six-wall physical protection where the ESP extends between PSPs, but URE had failed to file a TFE with Reliability*First*. In addition, URE discovered that two network switches that it previously represented as residing within a PSP did not actually reside in a documented PSP. These network switches are Cyber Assets within an ESP.

Based on the Self-Report, Reliability*First* determined that URE violated CIP-006-3 R1.1 for failure to ensure that all Cyber Assets within an ESP reside within an identified PSP.

Reliability*First* determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE moved the two network switches into the documented PSP.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed moderate risk to the reliability of the BPS because URE controls physical access to the sites containing the network switches through various accesses and monitoring methods. In addition, URE encrypts network traffic between PSPs within each ESP. The two network switches at issue resided in a physically-secured six-wall perimeter, for which URE had multiple levels of access in place for the relevant time period. Specifically, the two network switches were hidden in a locked room residing next to the documented PSP.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-006-3 R1.1 was submitted to Reliability*First* on April 18, 2011 with a proposed completion date of January 7, 2011. The Mitigation Plan was accepted by Reliability*First* on May 5, 2011, and approved by NERC on May 31, 2011. The Mitigation Plan for this violation is designated as MIT-10-3637 and was submitted as non-public information to FERC on June 3, 2011 in accordance with FERC orders.

According to the Mitigation Plan, URE:

1. Submitted a TFE to Reliability*First* regarding its network configuration that utilized an alternate method of six-wall physical protection where the ESP extends between PSPs; and

2. Immediately moved the two network switches into a documented PSP.

URE submitted a certification of completion for this Mitigation Plan to Reliability*First*, which stated that URE completed this mitigation plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. A document describing the Mitigation Plan to address the concerns identified in the Self-Report;
2. Certification of Mitigation Plan Completion signed by the senior manager indicates completion of the required Mitigation Plan;[12] and
3. The work orders completing the movement of fiber cable for the switches that were relocated to the NERC CIP PSP signed by the CCA owner.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-006-3 R1.1.[13]

**CIP-007-3 R1.1 (RFC201100735)**

CIP-007-3, Requirement R1 provides 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-007-3, 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.

[12] This Certification contains the TFE request reference submitted to Reliability*First* to address the alternate measures for addressing R1.1. This certification also addresses the relocation of the network switches into a documented NERC CIP PSP. Reliability*First* approved the TFE.
[13] The Standard in the Verification of Mitigation Plan Completion is listed as CIP-006-2 R1.

> **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.

CIP-007-3 R1.1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that during its internal audit, URE discovered that it failed to ensure that significant changes to existing Cyber Assets within the ESP did not adversely affect existing cyber security controls. Specifically, the testing that URE conducted pursuant to CIP-007-3 R1 did not determine whether the change would affect existing cyber security controls in the ESP. Rather, the testing focused on whether the Cyber Asset would continue to function after the application of a significant change.

In addition, URE discovered that its cyber security testing procedure did not specify that required testing should occur in a test environment rather than in a production environment. As a result, URE did not use a test environment during its testing, and failed to conduct its cyber security testing procedure in a manner that minimizes adverse effects on the production system or its operation.

Reliability*First* determined that URE violated CIP-007-3 R1.1 for failure to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls and by failing to create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

Reliability*First* determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because all assets at issue were located in a secured PSP to which a very limited number of individuals had access. All of those individuals with access to the PSP had NERC cyber security training and a valid PRA. All assets in question resided on isolated networks with no direct access to the corporate network or the internet, and all traffic to and from said networks traversed secured access points. As a result of the foregoing, Reliability*First* determined that it was less likely that the test procedures would adversely affect the production environment.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-007-3 R1.1 was submitted to Reliability*First* on April 18, 2011 with a proposed completion date of May 31, 2011. The Mitigation Plan accepted by

Reliability*First* on May 5, 2011 and approved by NERC on May 31, 2011. The Mitigation Plan for this violation is designated as MIT-10-3638 and was submitted as non-public information to FERC on June 3, 2011 in accordance with FERC orders.

According to the Mitigation Plan, URE:

1. Revised its procedures to remove any ambiguity regarding where and how testing should take place, and to ensure that there is a strong focus on whether a change would affect security controls in the ESP;

2. Conducted training and awareness regarding the revised procedures to ensure all personnel are aware of testing requirements; and

3. Implemented a uniform process for documenting testing.

URE submitted a certification of completion for this Mitigation Plan, which stated that URE completed this mitigation plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. A document detailing the activities required to mitigate the self reported violation;
2. Certification of Mitigation Plan Completion signed by the Senior Manager. The certification identifies the key milestone activities that were completed; and
3. A document that includes the original and revised test procedures. The revised test procedures illustrate completion of the mitigation plan.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-007-3 R1.1.

**CIP-007-3 R2 (RFC201100736)**

CIP-007-3 R2 provides in pertinent part: "Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled."

CIP-007-3 R2 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that during its internal audit, URE discovered that for 121 Cyber Assets, it failed to establish, document, and implement a process to ensure that it enables only those ports and services required for normal and emergency operations.

Based on the Self-Report, Reliability*First* determined that URE violated CIP-007-3 R2 for failure to establish, document and implement a process to ensure that it enables only those ports and services required for normal and emergency operations.

Reliability*First* determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE is expected to complete its Mitigation Plan.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because all assets at issue were located in a secured PSP to which a very limited number of individuals had access. All of those with access to the PSP had NERC cyber security training and a valid PRA. Therefore, it was less likely that an individual could accidentally or purposely access open ports and services and adversely affect URE's system. In addition, all assets in question resided on isolated networks with no direct access to the corporate network or the internet, and all traffic to and from said networks traversed secured access points, which included blocking well-known malicious traffic by port blocking at the access points. Therefore, Reliability*First* determined that it was less likely that an individual could tamper with URE's system through its ports and services. There is no evidence of malware on these devices.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-007-3 R2 was submitted to Reliability*First* on April 18, 2011 with a proposed completion date of October 31, 2011. The Mitigation Plan was accepted by Reliability*First* on May 5, 2011 and approved by NERC on May 31, 2011. The Mitigation Plan for this violation is designated as MIT-10-3639 and was submitted as non-public information to FERC on June 3, 2011 in accordance with FERC orders.

According to the Mitigation Plan, URE developed and implemented a vulnerability management assessment program. The vulnerability management assessment program documents URE's processes to ensure that it identifies, documents, and enables or disables all ports and services pursuant to the applicable Reliability Standards.

URE submitted a certification of completion for this Mitigation Plan, which stated that URE completed this mitigation plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Vulnerability management and assessment program;
2. Correspondences between URE and its vendor;
3. Complete list of ports that are required for normal and emergency operations broken down by host name;
4. Complete list of all installed services that are required for normal and emergency operation broken into Server2003 and Windows XP;
5. Ports and Services scan of the impacted devices;
6. Annual assessment to ensure the approved baseline is accurate;
7. Documentation related to services baseline and ports baseline that was established using the processed described in the vulnerability management and assessment program; and
8. Documentation of the scans performed to validate that the approved baseline reflects the actual environment.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-007-3 R2.

**CIP-007-3 R6.1 and R6.5 (RFC201100737)**

CIP-007-3 R6 provides in pertinent part:

> **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.
> >
> > **R6.5.** The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-3 R6 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First*, stating that it failed to configure its automated log monitoring to monitor all required devices. URE failed to monitor certain CCAs and Cyber Assets within the ESP for a couple of its registered functions. As a result, URE failed to review the logs of system events related to cyber security for those devices.

ReliabilityFirst determined that URE violated CIP-007-3 R6.1 and R6.5 for failure to implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the ESP and for failure to review logs of system events related to cyber security and maintain records documenting review of logs.

ReliabilityFirst determined the duration of the violation to be from the date URE was required to comply this Standard, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because all assets in question resided on isolated networks with no direct access to the corporate network, or the internet and all traffic to and from said networks traversed secured access points. URE blocked well-known malicious traffic by port blocking at the access point. As a result, ReliabilityFirst determined that it was less likely that a system event related to cyber security would occur.

In addition, all assets at issue were located in a secured PSP to which a very limited number of individuals had access. All of those individuals with access to the PSP had NERC cyber security training and a valid PRA. Therefore, ReliabilityFirst determined that it was less likely that a system event related to cyber security would not be noticed.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-007-3 R6.1 and R6.5 was submitted to ReliabilityFirst on April 18, 2011 with a proposed completion date of May 31, 2011. The Mitigation Plan was accepted by ReliabilityFirst on May 5, 2011 and approved by NERC on May 31, 2011. The Mitigation Plan for this violation is designated as MIT-10-3640 and was submitted as non-public information to FERC on June 3, 2011 in accordance with FERC orders.

According to the Mitigation Plan, URE combined all of its registered functions' processes for security status monitoring into one comprehensive security status monitoring program. The security status monitoring program addresses documentation of manual review of logs ensures that URE is monitoring all CCAs and Cyber Assets within the ESP, and clarifies roles and responsibilities.

URE certified completion for this Mitigation Plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. This document shows compilation of the newly created NERC-CIP security status monitoring program document;

2. Certification of Mitigation Plan Completion. signed by the senior manager; and
3. CIP-007 R6 Proposed Mitigation Plan Rev 2 of the Mitigation Plan.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-007-3 R6.

**VIOLATIONS DISCOVERED AT RELIABILITY*FIRST*'s COMPLIANCE AUDIT**

**CIP-005-3 R1.4 (RFC201100760)**

The purpose of Reliability Standard CIP-005-3 R1.4 provides: "Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-005-3 R1.4 provides 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).
>
> > **R1.4.** Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.

CIP-005-3 R1.4 has a "Medium" VRF and a "Severe" VSL.

Reliability*First* conducted a Compliance Audit of URE (Compliance Audit), during which Reliability*First* identified non-critical Cyber Assets within the ESP that URE failed to list as non-critical Cyber Assets within the ESP, as required by CIP-005-3 R1.4.[14] URE maintained a list that contained both CCAs and non-critical Cyber Assets within the ESP, but failed to identify all non-critical Cyber Assets within the ESP on that list.

Reliability*First* determined that URE violated CIP-005-3 R1.4 for failure to identify non-critical Cyber Assets within a defined ESP.

[14] The list at issue is the same document as the document at issue in the Self-Report of CIP-002-3 R3 (RFC201100733).

Reliability*First* determined the duration of the violation to be from the date that URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a minimal risk to the reliability of the BPS because although the list of non-critical Cyber Assets within the ESP was incomplete, URE separately maintained a list of non-critical Cyber Assets that was broader than the list initially approved by senior management. URE relied upon the broader, separately-maintained Cyber Assets list at all relevant times. In addition, URE protected the non-critical Cyber Assets within the ESP as though they were CCAs at all relevant times, affording those non-critical assets more protection than required by the CIP Standards.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-005-3 R1.4 was submitted to Reliability*First* on May 16, 2011 with a completion date of November 24, 2010. The Mitigation Plan accepted by Reliability*First* on June 7, 2011, and approved by NERC on July 5, 2011. The Mitigation Plan for this violation is designated as MIT-10-3787 and was submitted as non-public information to FERC on July 5, 2011 in accordance with FERC orders.

According to the Mitigation Plan, URE revised its lists of CCAs, Cyber Assets, and non-critical Cyber Assets within the ESP to reflect the production environment.

URE certified completion of this Mitigation Plan.
As evidence of completion of its Mitigation Plan, URE submitted the following:

1. manager document that illustrates that URE maintains a single control document included all relevant CCAs, Cyber Assets and non-critical Cyber Assets within the ESP;
2. Certification of a Completed Mitigation Plan signed by a NERC CIP Compliance Manager; and
3. CIP-005 R 1.4 Proposed Mitigation Plan, which is the actual Mitigation Plan.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-005-3 R1.4.

**CIP-005-3 R2.2 (RFC201100761)**

CIP-005-3 R2.2 provides in pertinent part:

R2. Electronic Access Controls – The Responsible 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).

> 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.

CIP-005-3 R2.2 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, Reliability*First* discovered a violation of CIP-005-3 R2.2 because URE utilizes four discrete ESPs as part of its SOC and a second Operations Center. These ESPs are interconnected using routers, which URE identified as access points to the ESPs. URE failed to demonstrate that it enabled only required ports and services for these routers. In addition, URE failed to document the configuration of the ports and services on these routers.

Reliability*First* determined that URE violated CIP-005-3 R2.2 for failure to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP and by failing to document the configuration of these ports and services.

Reliability*First* determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because each of the routers are configured only to allow communication with peers specifically defined in the router's configuration mapping. All peer routers are authenticated with one another based on a predefined and approved configuration, and all traffic is encrypted from router to router. Traffic through each encrypted tunnel is restricted to and from predefined destinations only. In addition, access control lists are in place to further define traffic origination and destination with a configuration to "deny all" traffic that does not meet a predefined access list parameter. All assets at issue were located in a secured PSP to which a very limited number of individuals had access. All of those individuals with access to the PSP had NERC cyber security training and a valid PRA.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-005-3 R2.2 was submitted to Reliability*First* on May 16, 2011 with a proposed completion date of June 30, 2011. The Mitigation Plan was accepted by Reliability*First* on June 7, 2011 and approved by NERC on July 5, 2011. The Mitigation Plan for this violation is designated as MIT-10-3788 and was submitted as non-public information to FERC on July 5, 2011 in accordance with FERC orders.

According to the Mitigation Plan URE enabled only required ports and services, and documented and validated that for all access points to the ESP, it enabled only required ports and services. In addition, URE documented the configuration of these ports and services.

URE certified completion for this Mitigation Plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. A document that provides a summary of the actions URE took to complete the mitigation plan and explains the contents of the other document submitted as evidence of verification.

Documents showing baseline ports and services for a listing of devices that comprise the ESP access points as identified by URE. Included with the documentation was a network diagram that identified PSPs, ESPs, and Cyber Assets constituting the access points to the ESPs.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-005-3 R2.2.

**CIP-005-3 R3.2 (RFC201100762)**

CIP-005-3 R3.2 provides in pertinent part:

> **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.

CIP-005-3 R3.2 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, Reliability*First* discovered a violation of CIP-005-3 R3.2 because URE had in place a deficient process for monitoring electronic access. While URE implemented logging for repeated unsuccessful login attempts, Reliability*First* determined that it failed to document and implement a process for alerting designated response personnel of attempts at unauthorized access or actual unauthorized accesses to the ESP.

As a result, Reliability*First* determined that URE violated CIP-005-3 R3.2 for failure to document and implement a security monitoring process that alerts designated response personnel of attempts at or actual unauthorized accesses to the ESP.

Reliability*First* determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because URE had logging in place during the time period of the violation, despite its failure to implement alerts. URE reviewed those logs manually, and discovered no attempts at unauthorized access. In addition, all assets at issue were located in a secured ESP and PSP to which a very limited number of individuals had access. As a result, Reliability*First* determined that it was less likely that an unauthorized individual could attempt to access the ESP. All of those individuals with access to the PSP had NERC cyber security training and a valid PRA.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-005-3 R3.2 was submitted to Reliability*First* on May 16, 2011 with a proposed completion date of June 30, 2011. The Mitigation Plan was accepted by Reliability*First* on June 7, 2011, and approved by NERC on July 5, 2011. The Mitigation Plan for this violation is designated as MIT-10-3789 and was submitted as non-public information to FERC on July 5, 2011 in accordance with FERC orders.

According to the Mitigation Plan URE:

1. Expanded its security status monitoring program to incorporate monitoring electronic access and implemented alerting for actual unauthorized access;
2. Enabled alerting for unauthorized login attempts;
3. Participated in a training program with its monitoring software vendor to ensure understanding of the capabilities of the software; and
4. Configured the access points to provide an additional alert for security events.

URE certified completion for this Mitigation Plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

NERC Compliance Certification of Mitigation Plan Completion submitted on June 17, 2011. This document provides a summary of the actions taken to complete the mitigation plan and provides an explanation of the contents of the other document submitted as evidence of verification.

1. A document that provides a summary of the actions taken to complete the mitigation plan and provides an explanation of the contents of the other document submitted as evidence of verification; Evidence that logging, monitoring and alerting are enabled on the firewall access points and sampled using an invalid login attempt that generates an e-mail notification;
2. A list of URE staff that were present for the training with the monitoring software vendor; and
3. A document that provides the procedure for monitoring and alerting for all access points to the ESP, all access points to an ESP and any system used in the access control and monitoring of the ESP.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-005-3 R3.2.

**CIP-005-3 R4.2 (RFC201100763)**

CIP-005-3 R4.2 provides in pertinent part:

> **R4.** Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

**R4.2.** A review to verify that only ports and services required for operations at these access points are enabled.

CIP-005-3 R4.2 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, Reliability*First* discovered a violation of CIP-005-3 R4.2 because URE annually performed a cyber vulnerability assessment of the electronic access points to the ESP but failed to include a review in its cyber vulnerability assessment to verify that it enabled only ports and services required for operations at the electronic access points to the ESP.

Reliability*First* determined that URE violated CIP-005-3 R4.2 for failure to include a review in its cyber vulnerability assessment to verify that it enabled only those ports and services required for operations at electronic access points to the ESP.

Reliability*First* determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because URE did not observe attempts at or actual unauthorized access during the time period of the violation. In addition, all assets at issue were located in a secured PSP to which a very limited number of individuals had access and an individual could not gain malicious access to the URE site. Also, all of those with access to the PSP had NERC cyber security training and a valid PRA.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-005-3 R4.2 was submitted to Reliability*First* on May 16, 2011 with a proposed completion date of June 30, 2011. The Mitigation Plan was accepted by Reliability*First* on June 7, 2011, and approved by NERC on July 5, 2011. The Mitigation Plan for this violation is designated as MIT-10-3790 and was submitted as non-public information to FERC on July 5, 2011 in accordance with FERC orders.

According to the Mitigation Plan, URE revised its comprehensive, enterprise-wide vulnerability management assessment program by incorporating a detailed process to review its lists of ports and services required for operations at electronic access points to the ESP.

URE certified completion for this Mitigation Plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. A document that provides a summary of the actions URE took to complete the mitigation plan and explains the contents of the other document submitted as evidence of verification, including a list of PDF files; and
2. Vulnerability management and assessment program; and
3. A document that consists of baselines for ports and services on specific devices and the approval of those baselines.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-005-3 R4.2.

**CIP-007-3 R2.1 (RFC201100764)**[15]

CIP-007-3 R2.1 provides in pertinent part:

> **R2.** Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> > **R2.1.**The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

CIP-007-3 R2.1 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, Reliability*First* determined that URE had a process in place to ensure that it enables only those ports and services required for normal and emergency operations at its facilities, but URE failed to enable only those ports and services required for normal and emergency operations.

As a result, Reliability*First* determined that URE violated CIP-007-3 R2.1 for failure to enable only those ports and services required for normal and emergency operations.

Reliability*First* determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.[16]

[15]Reliability*First* determined that this violation is related but separate from the violation of CIP-007-3 R2 (RFC201100736).
[16] In its Mitigation Plan, URE stated that it would complete the plan by October 31, 2011.

ReliabilityFirst determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because all assets at issue were located in a secured PSP to which a very limited number of individuals had access. All individuals with access to the PSP had NERC cyber security training and a valid PRA. As a result, ReliabilityFirst determined that it was less likely that an individual could accidentally or purposely access open ports and services and adversely affect URE's system.

In addition, all assets in question resided on isolated networks with no direct access to the corporate network or the internet, and all traffic to and from said networks traversed secured access points. Therefore, ReliabilityFirst determined that it was less likely that an individual could tamper with URE's system through its ports and services.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-007-3 R2.1 was submitted to ReliabilityFirst on April 18, 2011 with a proposed completion date of October 31, 2011. The Mitigation Plan was accepted by ReliabilityFirst on May 16, 2011 and approved by NERC on June 21, 2011. The Mitigation Plan for this violation is designated as MIT-10-3719 and was submitted as non-public information to FERC on June 23, 2011 in accordance with FERC orders.

According to the Mitigation Plan URE developed an enterprise-wide comprehensive vulnerability management assessment program. The program ensures that URE identifies, documents, and enables ports and services in accordance with the CIP Standards.

In its Mitigation Plan, URE stated that it is taking interim measures to address the issue while the Mitigation Plan is being implemented. URE currently has a vulnerability management assessment program in place, and the execution of the procedures in the program have produced no evidence of malicious or dangerous ports and service configuration/installation. URE stated that its subject matter experts are working diligently with its vendors and are evaluating the expansion of our labor force to document an accurate baseline. Also, URE's SOC is scheduled to have a system upgrade. The processes will be in place to ensure the baseline for the new devices is completed correctly prior to the installation of the system upgrade.

URE submitted a certification of completion for this Mitigation Plan, which stated that URE completed this mitigation plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Vulnerability management and assessment program;
2. Correspondences between URE and its vendor;

3. Complete list of ports that are required for normal and emergency operations broken down by host name;
4. Complete list of all installed services that are required for normal and emergency operation broken into Server2003 and Windows XP;
5. Ports and Services scan of the impacted devices;
6. Annual assessment to ensure the approved baseline is accurate;
7. Documentation related to services baseline and ports baseline that was established using the processed described in the vulnerability management and assessment program; and
8. Documentation of the scans performed to validate that the approved baseline reflects the actual environment.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-007-3 R2.

**CIP-007-3 R3. 1 and R3.2 (RFC201100765)**[17]

CIP-007-3 R3 provides:

> **R3.** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement 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.

CIP-007-3 R3 has a "Lower" VRF and a "Severe" VSL.

[17]This violation is related to the violation of CIP-007-3 R3 (RFC201100752) but Reliability*First* determined that it is a separate violation RFC201100752.

During the Compliance Audit, Reliability*First* discovered that URE utilized a device to perform vulnerability assessments on its system for its facilities and did not implement security patches unless the vulnerability appeared in the vulnerability assessment. URE did not configure the device with the necessary authorizations to evaluate URE's system, and as a result, the device found no vulnerabilities. URE failed to install any security patches from the time of mandatory compliance with the CIP Standards, and also failed to document compensating measures applied to mitigate risk exposure in the case where it failed to install patches.

Reliability*First* determined that URE violated CIP-007-3 R3.1 and R3.2 for failure to document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades and for failure to document compensating measures applied to mitigate risk exposure in any case where the patch is not installed.

Reliability*First* determined the duration of this violation to be from the date URE was required to comply with this Standard, through when URE is expected to complete its Mitigation Plan.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because URE had enabled local logging on the local device to track and retain logs of authenticated and unauthenticated events. In addition, all assets at issue were located in a secured PSP to which a very limited number of individuals had access to it. All of those with access to the PSP had NERC cyber security training and a valid PRA.

All assets in question resided on isolated networks with no direct access to the corporate network or the internet, and all traffic to and from said networks traversed secured access points, which had access rules that blocked known malicious traffic at the network perimeter. As a result, it was less likely that URE's system would be susceptible to malware.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-007-3 R3.1 and R3.2 was submitted to Reliability*First* on April 18, 2011 with a proposed completion date of January 31, 2012. The Mitigation Plan was accepted by Reliability*First* on May 16, 2011 and approved by NERC on June 21, 2011. The Mitigation Plan for this violation is designated as MIT-10-3720 and was submitted as non-public information to FERC on June 23, 2011 in accordance with FERC orders.

According to the Mitigation Plan, URE:

1. Ran authenticated scans of its devices in a test environment in order to determine whether the scanning would negatively impact its devices;

2. Will run authenticated scans of its devices in the production environment in order to determine applicable security patches and security upgrades;

3. Will then document the assessment of security patches and security upgrades; and

4. Will install a server upgrade which will allow the vendor to test, apply, and document the implementation of security patches and security upgrades. In cases where it cannot install a security patch, URE will document compensating measures applied to mitigate risk exposure.

URE submitted a certification of completion for this Mitigation Plan, which stated that URE completed this mitigation plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Documentation showing the authenticated scan of certain devices;
2. Final Windows workstation patch list;
3. The list of patches that the vendor applied to the Windows Servers;
4. The list of patches that were applied to the servers;
5. The assessment of the patches for the Windows Workstations;
6. Vulnerability management assessment program;
7. Documentation that demonstrate the patches that were implemented URE has provided the log file from the Windows Workstation used to create the image to apply to the remaining workstations;
8. Screenshots of the initial Windows Workstation's "Add or Remove Programs" menu;
9. The analysis of the patches not applied and a detailed reason why these patches did not apply;
10. Documentation of the implementation of patches applied to the Windows Server;
11. Export of all the patches that are on certain servers;
12. The list of subject matter experts used to validate patches that were implemented on each device.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-007-3 R2.

**CIP-007-3 R5.1.2, R5.1.3, and R5.3.2 (RFC201100766)**

CIP-007-3 R5 provides in pertinent part:

> **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.
> >
> > > **R5.1.2.**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.
> > >
> > > **R5.1.3.**The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.
> >
> > **R5.3.** At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:
> >
> > > **R5.3.2.** Each password shall consist of a combination of alpha, numeric, and "special" characters.

URE's violation of CIP-007-3 R5 implicated R5.1.2, which has a VRF of "Lower" and a VSL of "Moderate," R5.1.3, which has a VRF of "Medium" and a VSL of "Severe," and R5.3.2, which has a VRF of "Lower" and a VSL of "Severe."

During the Compliance Audit, Reliability*First* discovered that URE failed to maintain historical audit trails of individual user account access activity for a device within a facility ESP for a period of approximately two months. In addition, URE failed to annually review user accounts for a device at this facility. Reliability*First* determined that URE utilizes standard Microsoft Windows password complexity

rules, which are not compliant with the password requirements contained within CIP-007-3 R5.3.2. URE failed to submit a TFE for this Requirement.

Therefore, Reliability*First* determined that URE violated CIP-007-3 R5.1.2, R5.1.3 and R5.3.2 for failure to create historical audit trails of individual user account access activity for a minimum of ninety days, for failure to review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 R4, and for failure to submit a TFE for its password requirements.

Reliability*First* determined that the duration of violation of CIP-007-3 R5.1.2 was from October 26, 2010, the date URE failed to maintain historical audit trails on one device in the ESP, until December 14, 2010, the date URE resumed maintaining audit trails.

The duration of violation of CIP-007-3 R5.1.3 was from the date URE was required to comply with this Standard, to the date URE conducted the annual review. The duration of the violation of CIP-007-3 R5.3.2 is from the date URE was required to comply with this Standard, to the date URE submitted a TFE to Reliability*First*.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because URE maintained audit trails on the device with sufficient detail to create a historical audit trail of individual user account access activity with the exception of the time period at issue. In addition, URE conducted the proper review pursuant to R5.1.3 for all other devices, indicating that the violation of R5.1.3 was an isolated incident.

**Status of Mitigation Plan**

URE Mitigation Plan to address its violation of CIP-007-3 R5.1.2, R5.1.3 and R5.3.2 was submitted to Reliability*First* on April 18, 2011 as completed as of December 17, 2010. The Mitigation Plan was accepted by Reliability*First* on May 16, 2011 and approved by NERC on June 21, 2011. The Mitigation Plan for this violation is designated as MIT-10-3721 and was submitted as non-public information to FERC on June 23, 2011 in accordance with FERC orders.

According to the Mitigation Plan URE:

1. Configured its system to allow it to retain Security Event Logs for approximately 180 days and other Event Logs for specified periods of time;

2. Implemented this configuration within all of its sites containing CCAs;

3. Centralized the annual review process for verifying access privileges and performed the annual review; and

4. Submitted a TFE to Reliability*First* regarding the devices that utilize Microsoft Windows password complexity rules that did not address the password requirements contained within CIP-007-3 R5.3.2.

URE certified completion for this Mitigation Plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. A document demonstrating appropriately sized logs to store the required information as well as applicable reviews (R5.3.2);
2. R5.3.2 Certification of Completed Mitigation Plan signed by a URE NERC CIP Compliance Manager;
3. A document demonstrating appropriately sized logs to store the required information as well as applicable reviews (R5.1.3);
4. R5.1.3 Certification of Completed Mitigation Plan signed by a URE NERC CIP Compliance Manager;
5. A screen shot of URE's Technical Feasibility Exception (TFE) Part A submittal; and
6. R5.3.2 Certification of a Completed Mitigation Plan signed by a NERC CIP Compliance Manager.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-007-3 R5.1.2, R5.1.3 and R5.3.2.

**CIP-007-3 R8.2 (RFC201100767)**

CIP-007-3 R8.2 provides in pertinent part:

> **R8.** Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> > **R8.2.** A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled.

CIP-007-3 R8.2 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, Reliability*First* discovered that URE performed a cyber vulnerability assessment but failed to conduct a review to verify that it only enabled those ports and services required for operation of the Cyber Assets within the ESP.

Reliability*First* determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because all assets in question resided on isolated networks with no direct access to the corporate network or the internet, and all traffic to and from said networks traversed secured access points, which had access rules that blocked known malicious traffic at the network perimeter. Therefore, Reliability*First* determined that it was less likely that an individual could tamper with URE's system through its ports and services.

In addition, all assets at issue were located in a secured PSP to which a very limited number of individuals had access. All individuals with access to the PSP had NERC cyber security training and a valid PRA. Therefore, Reliability*First* determined that it was less likely that an individual could accidentally or purposely access open ports and services and adversely affect URE's system.

**Status of Mitigation Plan**

URE's Mitigation Plan to address its violation of CIP-007-3 R8.2 was submitted to Reliability*First* on April 18, 2011 with a proposed completion date of May 31, 2011. The Mitigation Plan was accepted by Reliability*First* on May 16, 2011 and approved by NERC on June 21, 2011. The Mitigation Plan for this violation is designated as MIT-10-3722 and was submitted as non-public information to FERC on June 23, 2011 in accordance with FERC orders.

According to the Mitigation Plan URE implemented a comprehensive, enterprise-wide Vulnerability Management Assessment Program, which includes the process of the review to verify it enabled only ports and services required for operation of the Cyber Assets within the ESP.

URE certified completion for this Mitigation Plan. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Vulnerability management assessment program;
2. A complete list of ports that are required for normal and emergency operation broken down by host name;
3. The Ports and Services scan of the impacted devices at URE's facilities; and

4. The Annual review of the ports and services baseline.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed with respect to CIP-007-3 R8.2.

**Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed** [18]

**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,[19] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on November 1, 2011. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of a one hundred and fifteen thousand dollar ($115,000) 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. Reliability*First* considered certain aspects of URE's compliance program to be a mitigating factor in the penalty determination;
2. Reliability*First* considered the following violations to be evidence of a broad deficiency in URE's Compliance Program:
    a. The violations of CIP-007-1 R2 (RFC201100736), R2.1 (RFC201100764); R3 (RFC201000452); R6 (RFC201000737); and R8.2 (RFC201100767), because they appear to have been caused by URE's lack of a comprehensive program and procedures relative to NERC CIP compliance. Therefore, Reliability*First* did not apply full mitigating credit for URE's NERC compliance program.
3. Reliability*First* applied mitigating credit for the violations that URE self-reported0;

[18] *See* 18 C.F.R. § 39.7(d)(4).
[19] *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).

4. Reliability*First* applied partial mitigating credit for certain violations that URE self-reported because they were discovered during the weeks leading up to the Compliance Audit;

5. Reliability*First* considered that it discovered eight of the violations at the Compliance Audit and did not apply mitigating credit for these violations;

6. Reliability*First* considered as a mitigating factor the positive degree and quality of URE's cooperation during the enforcement processes, and the fact that URE promptly submitted effective mitigation plans to remediate all violations.

7. The violations constituted URE's first occurrence of violations of the subject NERC Reliability Standards;[20]

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred and fifteen thousand dollars ($115,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote accountability and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty 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 Notice of Penalty are the following documents:

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

   a. URE's Self-Report for CIP-007-1 R3.1 and R3.2, R4.1, and R6, included as Attachment A to the Settlement Agreement;

   b. URE's Mitigation Plan designated as MIT-10-3094 for CIP-007-1 R3.1 and R3.2, R4.1, and R6, included as Attachment B to the Settlement Agreement;

   c. URE's Certification of Mitigation Plan Completion for CIP-007-1 R3, included as Attachment C to the Settlement Agreement;

[20]Although URE has multiple violations of CIP-007 R3 (RFC201000452 and RFC201100765); CIP-007 R6 (RFC201000454 and RFC201100737); and CIP-007 R2 (RFC201100736 and RFC201100764), these violations were occurring concurrently, and consequently, Reliability*First* did not consider these violations to be repetitive infractions.

d. URE's Certification of Mitigation Plan Completion for CIP-007-1 R4.1, included as Attachment D to the Settlement Agreement;

e. URE's Certification of Mitigation Plan Completion for CIP-007-1 R6, included as Attachment E to the Settlement Agreement;

f. URE's Self-Report for CIP-004-2 R4.2, included as Attachment F to the Settlement Agreement;

g. URE's Mitigation Plan designated as MIT-10-2859 for CIP-004-2 R4.2, included as Attachment G to the Settlement Agreement;

h. URE's Certification of Mitigation Plan Completion for CIP-004-2 R4.2, included as Attachment H to the Settlement Agreement;

i. Reliability*First* Verification of Mitigation Plan Completion for CIP-004-2 R4.2, included as Attachment I to the Settlement Agreement;

j. URE's Self-Report for CIP-002-3 R3.2, included as Attachment J to the Settlement Agreement;

k. URE's Mitigation Plan designated as MIT-10-3658 for CIP-002-3 R3.2, included as Attachment K to the Settlement Agreement;

l. URE's Certification of Mitigation Plan Completion for CIP-002-3 R3.2, included as Attachment L to the Settlement Agreement;

m. URE's Self-Report for CIP-006-3 R1.1, included as Attachment M to the Settlement Agreement;

n. URE's Mitigation Plan designated as MIT-10-3637 for CIP-006-3 R1.1, included as Attachment N to the Settlement Agreement;

o. URE's Certification of Mitigation Plan Completion for CIP-006-3 R1.1, included as Attachment O to the Settlement Agreement;

p. URE's Self-Report for CIP-007-3 R1.1, included as Attachment P to the Settlement Agreement;

q. URE's Mitigation Plan designated as MIT-10-3638 for CIP-007-3 R1.1, included as Attachment Q to the Settlement Agreement;

r. URE's Certification of Mitigation Plan Completion for CIP-007-3 R1.1, included as Attachment R to the Settlement Agreement;

s. URE's Self-Report for CIP-007-3 R2, included as Attachment S to the Settlement Agreement;

t. URE's Certification of Mitigation Plan Completion for CIP-007-3 R2, included as Attachment T to the Settlement Agreement;

u. URE's Self-Report for CIP-007-3 R6, included as Attachment U to the Settlement Agreement;

v. URE's Mitigation Plan designated as MIT-10-3640 for CIP-007-3 R6, included as Attachment V to the Settlement Agreement;

w. URE's Certification of Mitigation Plan Completion for CIP-007-3 R6, included as Attachment W to the Settlement Agreement;

x. Reliability*First*'s Summary of Possible Violation for CIP-005-3 R1.4, included as Attachment X to the Settlement Agreement;

y. URE's Mitigation Plan designated as MIT-10-3787 for CIP-005-3 R1.4, included as Attachment Y to the Settlement Agreement;

z. URE's Certification of Mitigation Plan Completion for CIP-005-3 R1.4, included as Attachment Z to the Settlement Agreement;

aa. Reliability*First*'s Summary of Possible Violation for CIP-005-3 R2.2, included as Attachment AA to the Settlement Agreement;

bb. URE's Mitigation Plan designated as MIT-10-3788 for CIP-005-3 R2.2, included as Attachment BB to the Settlement Agreement;

cc. URE's Certification of Mitigation Plan Completion for CIP-005-3 R2.2, included as Attachment CC to the Settlement Agreement;

dd. Reliability*First*'s Summary of Possible Violation for CIP-005-3 R3.2, included as Attachment DD to the Settlement Agreement;

ee. URE's Mitigation Plan designated as MIT-10-3789 for CIP-005-3 R3.2, included as Attachment EE to the Settlement Agreement;

ff. URE's Certification of Mitigation Plan Completion for CIP-005-3 R3.2, included as Attachment FF to the Settlement Agreement;

gg. Reliability*First*'s Summary of Possible Violation for CIP-005-3 R4.2, included as Attachment GG to the Settlement Agreement;

hh. URE's Mitigation Plan designated as MIT-10-3790 for CIP-005-3 R4, included as Attachment HH to the Settlement Agreement;

ii. URE's Certification of Mitigation Plan Completion for CIP-005-3 R4, included as Attachment II to the Settlement Agreement;

jj. Reliability*First*'s Summary of Possible Violation for CIP-007-3 R2.1, included as Attachment JJ to the Settlement Agreement;

kk. URE's Mitigation Plan designated as MIT-10-3719 for CIP-007-3 R2.1, included as Attachment KK to the Settlement Agreement;

ll. Reliability*First*'s Summary of Possible Violation for CIP-007-3 R3, included as Attachment LL to the Settlement Agreement;

mm. URE's Mitigation Plan designated as MIT-10-3720 for CIP-007-3 R3, included as Attachment MM to the Settlement Agreement;

nn. Reliability*First*'s Summary of Possible Violation for CIP-007-3 R5, included as Attachment NN to the Settlement Agreement;

oo. URE's Mitigation Plan designated as MIT-10-3721 for CIP-007-3 R5, included as Attachment OO to the Settlement Agreement;

pp. URE's Certification of Mitigation Plan Completion for CIP-007-3 R5, included as Attachment PP to the Settlement Agreement;

qq. Reliability*First*'s Summary of Possible Violation for CIP-007-3 R8.2, included as Attachment QQ to the Settlement Agreement;

rr. URE's Mitigation Plan designated as MIT-10-3722 for CIP-007-3 R8.2, included as Attachment OO to the Settlement Agreement;

ss. URE's Certification of Mitigation Plan Completion for CIP-007-3 R8.2, included as Attachment SS to the Settlement Agreement;

b) Reliability*First* Verification of Mitigation Plan Completion for CIP-007-1 R3, CIP-007-1 R4.1, and CIP-007-1 R6, included as Attachment b;

c) Reliability*First* Verification of Mitigation Plan Completion for CIP-002-3 R3, included as Attachment c;

d) Reliability*First* Verification of Mitigation Plan Completion for CIP-006-3 R1, included as Attachment d;

e) Reliability*First* Verification of Mitigation Plan Completion for CIP-007-3 R1, included as Attachment e;

f) Reliability*First* Verification of Mitigation Plan Completion for CIP-007-3 R2, included as Attachment f;

g) Reliability*First* Verification of Mitigation Plan Completion for CIP-007-3 R6, included as Attachment g;

h) Reliability*First* Verification of Mitigation Plan Completion for CIP-005-3 R1.4, included as Attachment h;

i) Reliability*First* Verification of Mitigation Plan Completion for CIP-005-3 R2.2, included as Attachment i;

j) Reliability*First* Verification of Mitigation Plan Completion for CIP-005-3 R3.2, included as Attachment j;

k) Reliability*First* Verification of Mitigation Plan Completion for CIP-005-3 R4.2, included as Attachment k;

l) URE's Certification of Mitigation Plan Completion for CIP-007-3 R2.1, included as Attachment l;

m) Reliability*First* Verification of Mitigation Plan Completion for CIP-007-3 R2.1, included as Attachment m;

n) URE's Certification of Mitigation Plan Completion for CIP-007-3 R3, included as Attachment n;

o) Reliability*First* Verification of Mitigation Plan Completion for CIP-007-3 R3, included as Attachment o;

p) Reliability*First* Verification of Mitigation Plan Completion for CIP-007-3 R5, included as Attachment p; and

q) Reliability*First* Verification of Mitigation Plan Completion for CIP-007-3 R8.2, included as Attachment q.

**A Form of Notice Suitable for Publication**[21]

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

[21] *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<br>President and Chief Executive Officer<br>North American Electric Reliability Corporation<br>3353 Peachtree Road NE<br>Suite 600, North Tower<br>Atlanta, GA 30326-1001<br><br>David N. Cook*<br>Senior Vice President and General Counsel<br>North American Electric Reliability Corporation<br>1325 G Street N.W., Suite 600<br>Washington, D.C. 20005<br>david.cook@nerc.net<br><br>Megan E. Gambrel*<br>Attorney<br>Reliability*First* Corporation<br>320 Springside Drive, Suite 300<br>Akron, OH 44333<br>(330) 456-2488<br>megan.gambrel@rfirst.org<br><br>Michael D. Austin*<br>Managing Enforcement Attorney<br>Reliability*First* Corporation<br>320 Springside Drive, Suite 300<br>Akron, OH 44333<br>(330) 456-2488<br>mike.austin@rfirst.org<br><br>*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*<br>Associate General Counsel for Corporate and Regulatory Matters<br>Davis Smith*<br>Attorney<br>North American Electric Reliability Corporation<br>1325 G Street N.W., Suite 600<br>Washington, DC 20005<br>(202) 393-3998<br>(202) 393-3955 – facsimile<br>rebecca.michael@nerc.net<br>davis.smith@nerc.net<br><br>Robert K. Wargo*<br>Director of Enforcement<br>Reliability*First* Corporation<br>320 Springside Drive, Suite 300<br>Akron, OH 44333<br>(330) 456-2488<br>bob.wargo@rfirst.org<br><br>L. Jason Blake*<br>General Counsel<br>Reliability*First* Corporation<br>320 Springside Drive, Suite 300<br>Akron, OH 44333<br>(330) 456-2488<br>jason.blake@rfirst.org |

**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*

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Davis Smith
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
davis.smith@nerc.net

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, D.C. 20005
david.cook@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

Attachments