PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

December 31, 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 1, Unidentified Registered Entity 2, and Unidentified Registered Entity 3**
**FERC Docket No. NP13-_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), NERC Registry ID# NCRXXXXX, Unidentified Registered Entity 2 (URE2), NERC Registry ID# NCRXXXXX, and Unidentified Registered Entity 3 (URE3), NERC Registry ID# NCRXXXXX, (collectively, the UREs) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

The UREs submitted Self-Reports for the violations addressed below. The UREs operate from the same control room and share the same energy management system (EMS). As a result, the conduct addressed below relates to the shared EMS and constitutes 21 violations by the UREs of seven Reliability Standard Requirements.

This Notice of Penalty is being filed with the Commission because Reliability*First* Corporation (Reliability*First*) and the UREs have entered into a Settlement Agreement to resolve all outstanding

[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).

issues arising from Reliability*First*'s determination and findings of the violations[3] of CIP-005-3 R1/1.5 and R2;[4] CIP-005-2 R4/4.2;[5] CIP-006-3 R2/2.2;[6] and CIP-007-3 R2, R3 and R8.[7]

According to the Settlement Agreement, the UREs neither admit nor deny the violations, but have agreed to the assessed penalty of eighty thousand dollars ($80,000), 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 RFC201100785, RFC201100795, RFC201100805, RFC201100786, RFC201100796, RFC201100806, RFC201100787, RFC201100797, RFC201100807, RFC201100788, RFC201100798, RFC201100808, RFC201100790, RFC201100800, RFC201100809, RFC201100791, RFC201100801, RFC201100810, RFC201100794, RFC201100804 and RFC201100813 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, by and between Reliability*First* and the UREs, 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 (2012), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.
[4] The durations of the CIP-005-3 R1.5 and R2 violations also include Versions 1 and 2 of the Standard. This Full Notice of Penalty will refer only to Version 3 for consistency.
[5] The durations of the CIP-005-2 R4 violations also include Version 1 of the Standard. This Full Notice of Penalty will refer only to Version 2 for consistency.
[6] The durations of the CIP-006-3 R2.2 violations also include Versions 1 and 2 of the Standard. This Full Notice of Penalty will refer only to Version 3 for consistency. When CIP-006-2 became effective, the "Cyber Assets used in the access control and monitoring of the Physical Security Perimeter" from CIP-006-1 R1.8 became "Cyber Assets that authorize and/or log access to the Physical Security Perimeter" in CIP-006-2 R2. The Settlement Agreement and Full Notice of Penalty use the terminology from CIP-006-3 R2.2 throughout, and where applicable, it designates the language from CIP-006-1 R1.8.
[7] The durations of the CIP-007-3 R2, R3 and R8 violations also include Versions 1 and 2 of the Standard. This Full Notice of Penalty will refer only to Version 3 for consistency.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

| Region | NOC ID | Registered Entity Acronym | NERC Violation ID | Reliability Std. | Req. (R) | VRF/ VSL | Total Penalty |
|---|---|---|---|---|---|---|---|
| ReliabilityFirst Corporation | NOC-1406 | URE2 | RFC201100785 | CIP-005-3 | R1/1.5 | Medium/ Severe | $80,000 |
| | | URE1 | RFC201100795 | | | | |
| | | URE3 | RFC201100805 | | | | |
| | | URE2 | RFC201100786 | CIP-005-3 | R2 | Medium/ Severe | |
| | | URE1 | RFC201100796 | | | | |
| | | URE3 | RFC201100806 | | | | |
| | | URE2 | RFC201100787 | CIP-005-2 | R4/4.2 | Medium/ Severe | |
| | | URE1 | RFC201100797 | | | | |
| | | URE3 | RFC201100807 | | | | |
| | | URE2 | RFC201100788 | CIP-006-3 | R2/2.2 | Medium/ Severe | |
| | | URE1 | RFC201100798 | | | | |
| | | URE3 | RFC201100808 | | | | |
| | | URE2 | RFC201100790 | CIP-007-3 | R2 | Medium/ Severe | |
| | | URE1 | RFC201100800 | | | | |
| | | URE3 | RFC201100809 | | | | |
| | | URE2 | RFC201100791 | CIP-007-3 | R3 | Lower/ Severe | |
| | | URE1 | RFC201100801 | | | | |
| | | URE3 | RFC201100810 | | | | |
| | | URE2 | RFC201100794 | CIP-007-3 | R8 | Lower/ Severe | |
| | | URE1 | RFC201100804 | | | | |
| | | URE3 | RFC201100813 | | | | |

CIP-005-3 R1.5 (URE2: RFC201100785, URE1: RFC201100795, and URE3: RFC201100805)

The purpose statement of Reliability Standard CIP-005-3 provides in pertinent part: "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."

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

CIP-005-3 R1.5 provides:

> R1. Electronic Security Perimeter — The Responsible Entity[8] 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).
>
> *****
>
> R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

CIP-005-3 R1.5 has a "Medium" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

The UREs submitted a Self-Report to Reliability*First* identifying violations of CIP-005-3 R1.5. The UREs discovered that they failed to afford certain of their Cyber Assets used in the access control and monitoring of the Electronic Security Perimeters (ESPs) the protective measures specified in all CIP Standards listed, as required by CIP-005-3 R1.5.

Three of the UREs' Cyber Assets used in the access control and monitoring of the ESP are at issue. The first Cyber Asset provides access control and monitoring at all ESPs; the second Cyber Asset at issue is a server which provides access control and monitoring to another Cyber Asset device (which is within an ESP); and the third Cyber Asset at issue provides access control and monitoring to a network (which is within an ESP) (collectively, the Devices). The UREs failed to afford the Devices the protective measures as required by CIP-005-3 R1.5.

For all of the Devices, the UREs failed to afford the protections of CIP-005 R2.2 and CIP-007-3 R3 and R8. The UREs did not have documentation to show that only the required ports and services were enabled, as required by CIP-005-3 R2.2. In addition, the UREs failed to document the assessment and implementation of security patches for the Devices, as required by CIP-007-3 R3.1 and R3.2. The UREs

[8] Within the text of Standard CIP-002-CIP009, "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.

also failed to include a review of ports and services for these access control and monitoring Devices in their annual cyber vulnerability assessments for a particular year, as required by CIP-007-3 R8.2. For only the first and second devices, the UREs failed to afford the protection of CIP-003-3 R6 by failing to document that they followed their established change control and configuration management procedures for adding, modifying, replacing, or removing Critical Cyber Asset (CCA) hardware or software. For only the first device, the UREs failed to afford the protections of CIP-005-3 R2.6 and CIP-007-3 R1 and R5.1.1. Specifically, the UREs failed to implement banners in certain instances on the first device, as required by CIP-005-3 R2.6. In addition, the UREs had no documents to verify testing of security configurations in certain instances of significant changes to and the addition of certain new equipment, as required by CIP-007-3 R1 and R1.3. The UREs also granted an individual logical access to the integrated third device for a three-month period without ensuring approval by the designated personnel as required by CIP-007-3 R5.1.1.

Reliability*First* determined that the UREs had violations of CIP-005-3 R1.5 by failing to afford three Cyber Assets used in the access control and monitoring of the ESPs the protective measures as specified in Standards CIP-003, CIP-005 and CIP-007.

Reliability*First* determined the duration of the violations to be from the dates the UREs' were required to comply with CIP-005-1, through the date the UREs completed their Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. A violation of CIP-005-1 R1.5 has the potential to affect the reliable operation of the BPS by providing the opportunity for cyber intrusions to occur on CCAs located outside an established ESP. Specifically, the risk to the reliability of the BPS was mitigated by the following factors. The UREs do not utilize any of the systems at issue in these violations to operate and control Critical Assets. In addition, the ports and services that the UREs enabled beyond those which were necessary were only open for communications from other trusted corporate networks. Moreover, the UREs' trusted corporate networks were protected by firewalls, virtual local area network constraints, and domain and local account security restrictions at all relevant times. These protections illustrate a defense-in-depth strategy of protection that an intruder would have to overcome to gain access to the UREs' transmission management system.

CIP-005-3 R2 (URE2: RFC201100786, URE1: RFC201100796, and URE3: RFC201100806)
CIP-005-3 R2 provides in pertinent part:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> *****
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
>
> *****
>
> R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

CIP-005-3 R2 and R2.2 have a "Medium" VRF and CIP-005-3 R2.6 has a "Lower" VRF. These violations have a "Severe" VSL.

The UREs submitted a Self-Report to Reliability*First* identifying violations of CIP-005-3 R2. The UREs discovered that they failed to implement all electronic access controls at all electronic access points to the ESP. The UREs had no documentation to prove that only ports and services required for operations and monitoring of Cyber Assets at the access points to the ESP were enabled, in violation of CIP-005-3 R2.2. In addition, the UREs failed to maintain a formal document identifying the content of appropriate use banners, in violation of CIP-005-3 R2.6.

Reliability*First* determined that the UREs had violations of CIP-005-3 R2 by failing 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 those ports and services, and failing to maintain a document identifying the content of their appropriate use banner.

Reliability*First* determined the duration of the violations to be from the dates the UREs were required to comply with CIP-005-1, through for R2.6, the date appropriate use banners were formally documented and through for R2.2, the date the UREs enabled only ports and services required for operations and monitoring Cyber Assets within the ESP.

ReliabilityFirst determined that these violations posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. NERC, based on evaluation of the facts and circumstances of these violations and similar violations from other regional entities, determined that these violations posed a minimal risk to the reliability of the BPS. Specifically, the risk to the reliability of the BPS was mitigated by the following factors. For CIP-005-3 R2.2, the additional ports and services that the UREs enabled were only open from trusted corporate networks. In addition, the UREs' trusted corporate networks were protected by firewalls, virtual local area network constraints, and domain and local account security restrictions at all relevant times. These protections illustrate a defense-in-depth strategy of protection that an intruder would have to overcome to gain access to the UREs' transmission management system. In addition, for CIP-005-3 R2.6, the UREs were utilizing logon banners during the time period of the violations but had failed to document the content of the logon banners.

CIP-005-2 R4.2 (URE2: RFC201100787, URE1: RFC201100797, and URE3: RFC201100807)

The purpose statement of Reliability Standard CIP-005-2 provides in pertinent part: "Standard CIP-005-2 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-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2."

CIP-005-2 R4.2 provides:

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

The UREs submitted a Self-Report to ReliabilityFirst identifying violations of CIP-005-2 R4.2. The UREs performed a cyber vulnerability assessment of the electronic access points to the ESP in a particular year, but failed to include a review to verify that they enabled only ports and services required for operations at such access points.

ReliabilityFirst determined that the UREs had violations of CIP-005-2 R4.2 by failing to include a review in their annual cyber vulnerability assessment verifying that they enabled only ports and services required for operations.

ReliabilityFirst determined the duration of the violations to be from the dates the UREs' were required to comply with CIP-005-1, through the date the UREs completed their next annual cyber vulnerability assessment.

ReliabilityFirst determined that these violations posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. NERC, based on evaluation of the facts and circumstances of these violations and similar violations from other regional entities, determined that these violations posed a minimal risk to the reliability of the BPS. Upon review of the enabled ports and services, the UREs discovered they enabled certain ports and services not required for operations, which provides the opportunity for infiltration of unauthorized network traffic into the ESP through ports and services that are not necessary for normal or emergency operations but nevertheless remain enabled. However, the additional ports and services that the UREs enabled but were not required for operations and monitoring of Cyber Assets within the ESP were only open from trusted corporate networks. In addition, the UREs' trusted corporate networks were protected by firewalls, virtual local area network constraints, and domain and local account security restrictions at all relevant times. These protections illustrate a defense-in-depth strategy of protection that an intruder would have to overcome to gain access to the UREs' transmission management system.

CIP-006-3 R2.2 (URE2: RFC201100788, URE1: RFC201100798, and URE3: RFC201100808)

The purpose statement of Reliability Standard CIP-006-3 provides in pertinent part: "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 R2.2 provides:

> R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
>
> *****
>
> R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and

R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

CIP-006-3 R2 has a "Medium" VRF and a "Severe" VSL.

The UREs submitted a Self-Report to Reliability*First* identifying violations of CIP-006-3 R2.2. The UREs discovered that they (a) failed to afford, or (b) had incomplete documentation to support that they afforded certain of their Cyber Assets that authorize and/or log access to the Physical Security Perimeter (PSP) the protective measures specified in several CIP Standards listed in CIP-006-3 R2.2.

Two of the UREs' Cyber Assets that authorize and log access to the PSP are at issue. These include certain security system controls and logs access via cyber keys at PSPs, and another system controls and logs access via access cards at PSPs (collectively, the Physical Security Servers). The UREs failed to afford both of the Physical Security Servers the protective measures specified in CIP-003 R6; CIP-005 R2.2; and CIP-007 R1.3, R2, R3, R5.2.3, R5.3.3, R6.5, and R8.2.

The UREs failed to have a documented process for change control and configuration management for adding, modifying, replacing, or removing CCA hardware or software, as required by CIP-003-3 R6. In addition, the UREs failed to enable only required ports and services, as required by CIP-005-3 R2.2. The UREs failed to document cyber security test results in some instances of significant changes to existing Cyber Assets, as required by CIP-007-3 R1 and R1.3. The UREs failed to enable only required ports and services, as required by CIP-007-3 R2 (R2.1; R2.2; and R2.3). The UREs failed to have documentation regarding security patch assessments and compensating measures to mitigate risk exposure, as required by CIP-007-3 R3.1 and R3.2. The UREs failed to maintain audit trails of the account use of a shared account, as required by CIP-007-3 R5.2.3. The UREs failed to change user account passwords on an annual basis, as required by CIP-007-3 R5.3.3. The UREs failed to review logs of system events related to cyber security, as required by CIP-007-3 R6.5. Finally, the UREs failed to include a review of required ports and services in its cyber vulnerability assessment, as required by CIP-007-3 R8.2.

Regarding only the first security system, the UREs failed to afford the protections of CIP-005-3 R2.6, CIP-007-3 R4, and CIP-007-3 R5.2.1. The UREs failed to display banners on the user login screen, as required by CIP-005-3 R2.6. In addition, the UREs failed to have anti-virus software installed, as required by CIP-007-3 R4. The UREs also failed to change a factory default generic account password prior to placing the system into service, as required by CIP-007-3 R5.2.1.

Regarding only the second system, the UREs failed to afford the protections of CIP-007-3 R6.1. The UREs failed to document or implement a process to monitor PSP server security event logs, as required by CIP-007-3 R6.1.

Reliability*First* determined that the UREs had violations of CIP-006-3 R2.2 by failing to afford Cyber Assets that authorize and log access to the PSP the protective measures specified in CIP-003, CIP-005, and CIP-007.

Reliability*First* determined the duration of the violations to be from the dates the UREs were required to comply with CIP-006-1, through when the UREs completed their Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to implement operational and procedural controls to manage access to PSP could allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets. The ports and services at issue were only open to trusted corporate networks. In addition, the UREs' trusted corporate networks were protected by firewalls, virtual local area network constraints, and domain and local account security restrictions at all relevant times. These protections illustrate a defense-in-depth strategy of protection that an intruder would have to overcome to gain access to the UREs' transmission management system.

CIP-007-3 R2 (URE2: RFC201100790, URE1: RFC201100800, and URE3: RFC201100809)

The purpose statement of Reliability Standard CIP-007-3 provides in pertinent part: "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 Standards CIP-002-3 through CIP-009-3."

CIP-007-3 R2 provides:

> 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.

> R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
>
> R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

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

The UREs submitted a Self-Report to Reliability*First* identifying violations of CIP-007-3 R2. The UREs had a documented process to address those ports and services to be enabled for normal and emergency operations. The UREs discovered that they failed to implement that process to ensure that they only enable those ports and services required for normal and emergency operations, in violation of CIP-007-3 R2. As a result, the UREs failed to enable only ports and services required for normal and emergency operations, in violation of CIP-007-3 R2.1. In addition, the UREs failed to disable other ports and services prior to the production use of all Cyber Assets inside the ESP, in violation of CIP-007-3 R2.2. The UREs also failed to document compensating measures applied to mitigate risk exposure in the case where they could not disable unused ports and services, in violation of CIP-007-3 R2.3.

Reliability*First* determined that the UREs had violations of CIP-007-3 R2 by failing to implement a process to ensure that they enable only those ports and services required for normal and emergency operations.

Reliability*First* determined the duration of the violations to be from the dates the UREs were required to comply with CIP-007-1, through when the UREs finalized all required documentation and completed their Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Upon review of the enabled ports and services, the UREs discovered they enabled certain ports and services not required for operations, which provides the opportunity for infiltration of unauthorized network traffic into the ESP through ports and services that are not necessary for normal or emergency operations but nevertheless remain enabled. The additional ports and services that the UREs enabled were only open from trusted corporate networks. In addition, the UREs' trusted corporate networks were protected by firewalls, virtual local area network constraints, and domain and local account security restrictions at all relevant times. These

protections illustrate a defense-in-depth strategy of protection that an intruder would have to overcome to gain access to the UREs' transmission management system.

CIP-007-3 R3 (URE2: RFC201100791, URE1: RFC201100801, and URE3: RFC201100810)
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.

The UREs submitted a Self-Report to Reliability*First* identifying violations of CIP-007 R3. The UREs have a security patch management program in place, however, for their transmission management system they failed to fully document patch assessments and compensating measures applied to mitigate risk exposure when a patch is not installed. A vendor performed all assessments of security patches and upgrades within thirty days and supplied that information to the UREs for review.

The UREs failed to document their assessment of security patches and failed to document completely the implementation of security patches pursuant to their security patch management program, in violation of CIP-007-3 R3.1 and R3.2.

For the UREs' security protection systems, the UREs failed to have in place a tracking mechanism to monitor or record the thirty-day period allowed for analysis of the required network infrastructure software updates, in violation of CIP-007-3 R3.1. For devices within a certain group, the UREs failed to have in place a tracking mechanism to monitor or record the thirty-day period allowed for analysis of

the required firmware updates, in violation of CIP-007-3 R3.1. For the physical security access control and monitoring devices, the UREs failed to have in place a tracking mechanism to monitor or record the thirty-day period allowed for analysis of the required software updates, in violation of CIP-007-3 R3.1.

Reliability*First* determined that the UREs had violations of CIP-007-3 R3 by failing to document the assessment of security patches and security upgrades for applicability within thirty calendar days, and by failing to document the implementation of such patches and upgrades.

Reliability*First* determined the duration of the violations to be from dates the UREs were required to comply with CIP-007-1, through the date the UREs completed their Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Failure to document patch assessments and implementation, combined with the failure to document compensating measures applied to mitigate risk exposure, increase the potential risk to the BPS. The UREs mitigated this risk because all required security patches and security upgrades were implemented. In addition, the UREs' vendor performed the requisite assessments, and the UREs reviewed the vendor's assessments and partially documented that review.

CIP-007-3 R8 (URE2: RFC201100794, URE1: RFC201100804, and URE3: RFC201100813)
CIP-007-3 R8 provides:

> 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:
>
> R8.1. A document identifying the vulnerability assessment process;
>
> 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;
>
> R8.3. A review of controls for default accounts; and,
>
> R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

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

The UREs submitted a Self-Report to Reliability*First* identifying violations of CIP-007-3 R8. The UREs discovered that they failed to conduct a cyber vulnerability assessment of all Cyber Assets within the ESPs for a certain year. Though the UREs performed a cyber vulnerability assessment, the assessment did not include Cyber Assets within the ESPs. The UREs also failed to include a review to verify that they included only ports and services required for operation of the Cyber Assets within the ESP, in violation of CIP-007-3 R8.2.

Reliability*First* determined that the UREs had violations of CIP-007-3 R8 by failing to perform a cyber vulnerability assessment of all Cyber Assets within the ESP, and by failing to include in its cyber vulnerability assessment of all Cyber Assets within the ESP, a review to verify that only ports and services required for operation of the Cyber Assets within the ESP were enabled.

Reliability*First* determined the duration of the violations to be from the dates the UREs' were required to comply with CIP-007-1, through when the UREs completed the analysis of ports and services as part of the next annual cyber vulnerability assessment.

Reliability*First* determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Upon review of the enabled ports and services, the UREs discovered they enabled certain ports and services not required for operations, which provides the opportunity for infiltration of unauthorized network traffic into the ESP through ports and services that are not necessary for normal or emergency operations but nevertheless remain enabled. The Cyber Assets within the ESP, however, are only accessible from trusted corporate networks. In addition, the UREs' trusted corporate networks were protected by firewalls, virtual local area network constraints, and domain and local account security restrictions at all relevant times. These protections illustrate a defense-in-depth strategy of protection that an intruder would have to overcome to gain access to the UREs' transmission management system

Regional Entity's Basis for Penalty

According to the Settlement Agreement, Reliability*First* has assessed a penalty of eighty thousand dollars ($80,000) for the referenced violations. In reaching this determination, Reliability*First* considered the following factors:

1. The violations constituted the UREs' first occurrence of violations of the subject NERC Reliability Standards;

2. The UREs self-reported the violations;
3. Reliability*First* reported that the UREs were cooperative throughout the compliance enforcement process;
4. The UREs had a compliance program at the time of the violations which Reliability*First* considered a mitigating factor;
5. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. Reliability*First* determined that the violations posed a moderate and not a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. Reliability*First* reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, Reliability*First* determined that, in this instance, the penalty amount of eighty thousand dollars ($80,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

**Status of Mitigation Plans**[9]

**CIP-005-3 R1.5 URE2: RFC201100785, URE1: RFC201100795, and URE3: RFC201100805**

The UREs' Mitigation Plan to address the violations of CIP-005-3 R1.5 was submitted to Reliability*First* on December 14, 2011. The Mitigation Plan was accepted by Reliability*First* on January 6, 2012 and approved by NERC on January 18, 2012. The Mitigation Plan for the violations is designated as RFCMIT006479 and was submitted as non-public information to FERC on January 20, 2012 in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to take actions to address the violations of CIP-005-3 R1.5 by providing the protections specified by the referenced and applicable Reliability Standard Requirements, specifically:

1. To address CIP-003-3 R6, the UREs enhanced their change control documentation procedures by training individuals to use a change management tool to enter all change requests. The change management tool incorporates an approval workflow, testing steps, and all activity related to the change;

[9] *See* 18 C.F.R § 39.7(d)(7).

2. To address CIP-005-3 R2.2, the UREs analyzed their ports and services as part of its annual cyber vulnerability assessment, to ensure that only required ports and services are enabled at the ESP access points. The UREs will utilize the annual cyber vulnerability assessment, along with the revised change management process, to ensure that only required ports and services are enabled in the future;
3. To address CIP-005-3 R2.6, the UREs created, documented, and implemented a standard providing for logon banner language where technically feasible;
4. To address CIP-007-3 R1 and R1.3, the UREs performed testing to determine the necessary configuration changes required due to enabling only required ports and services. The UREs implemented a standard configuration for all applicable CCAs. In addition, the revised change control procedure includes significant changes to the standard configuration.
5. To address CIP-007-3 R3.1 and R3.2, the UREs updated their security patch management policy to include processes for:
    a. Newly released security patches;
    b. The tracking of the analysis of the patches;
    c. The determination to implement or not to implement the patch; and
    d. Documentation of the information.
6. To address CIP-007-3 R8.2, the UREs included ports and services for the first and second devices in the annual cyber vulnerability assessment. The second device was decommissioned the following year.

The UREs certified that the above Mitigation Plan requirements were completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that the UREs' Mitigation Plan was completed.

**CIP-005-3 R2 (URE2: RFC201100786, URE1: RFC201100796, and URE3: RFC201100806)**

The UREs' Mitigation Plan to address the violations of CIP-005-3 R2 was submitted to Reliability*First* on October 25, 2011. The Mitigation Plan was accepted by Reliability*First* on December 28, 2011 and approved by NERC on February 13, 2012. The Mitigation Plan for the violations is designated as RFCMIT006012 and was submitted as non-public information to FERC on February 14, 2012 in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to:

1. Perform an annual cyber vulnerability assessment, during which they conducted a review of the required ports and services at the access points to the ESPs and compared the results to actual ports and services at the access points to the ESPs;
2. Make configuration changes to the access control lists of the access points to the ESPs to enable access only to the required ports and services;
3. Continue to utilize the annual cyber vulnerability assessment process to determine which ports and services are required;
4. Address incremental changes to the ports and services through a change management process, which will ensure that only required ports and services are enabled; and
5. Standardize the logon banner language and document and implement it where technically feasible.

The UREs certified that the above Mitigation Plan requirements were completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that the UREs' Mitigation Plan was completed.

**CIP-005-2 R4.2 (URE2: RFC201100787, URE1: RFC201100797, and URE3: RFC201100807)**

The UREs' Mitigation Plan to address the violations of CIP-005-2 R4.2 was submitted to Reliability*First* on October 25, 2011. The Mitigation Plan was accepted by Reliability*First* on December 28, 2011 and approved by NERC on February 13, 2012. The Mitigation Plan for the violations is designated as RFCMIT006013 and was submitted as non-public information to FERC on February 14, 2012 in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to:

1. Perform an annual cyber vulnerability assessment, during which they are to conduct a review of the required ports and services at the access points to the ESPs and compare the results to actual ports and services at the access points to the ESPs;
2. Make configuration changes to the access control lists of the access points to the ESPs to enable access only to the required ports and services;

3. Continue to utilize the annual cyber vulnerability assessment process to determine which ports and services are required; and
4. Address incremental changes to the ports and services through a change management process, which will ensure that only required ports and services are enabled.

The UREs certified that the above Mitigation Plan requirements for RFC201100787 were completed. The UREs certified that the above Mitigation Plan requirements were completed for RFC201100797 and RFC201100807. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that the UREs' Mitigation Plan was completed.

**CIP-006-3 R2.2 (URE2: RFC201100788, URE1: RFC201100798, and URE3: RFC201100808)**

The UREs' Mitigation Plan to address the violations of CIP-006-3 R2.2 was submitted to Reliability*First* on December 14, 2011. The Mitigation Plan was accepted by Reliability*First* on January 6, 2012 and approved by NERC on February 10, 2012. The Mitigation Plan for the violations is designated as RFCMIT006480 and was submitted as non-public information to FERC on February 14, 2012 in accordance with FERC orders.

The UREs' Mitigation Plan listed the following activities the UREs took to mitigate the violation:

1. To address CIP-003-3 R6, the UREs revised the change control management system to capture significant changes for the Physical Security Servers;
2. To address CIP-005-3 R2.2, the UREs performed an annual cyber vulnerability assessment, during which they conducted a review to ensure only the required ports and services were enabled.
3. To address CIP-005-3 R2.6, the UREs implemented logon banners for the Physical Security Servers;
4. To address CIP-007-3 R1 and R1.3, the UREs track all significant changes to the Physical Security Servers with the change control management system;
5. To address CIP-007-3 R2, R2.1, R2.2 and R2.3, the UREs enabled only required ports and services, and disabled all ports and services not required. For those ports and services that are not required and cannot be disabled, the UREs implemented compensating measures;

6. To address CIP-007-3 R3, R3.1 and R3.2, the UREs recorded security patch assessments for the Physical Security Servers in the change control management tool;
7. To address CIP-007-3 R4, the UREs tested, documented, and installed anti-virus software and updates on the Physical Security Servers;
8. To address CIP-007-3 R5.2.1, the UREs changed the passwords for the Physical Security Servers and added a clear description of the password change process for shared accounts to their account management and logging policy;
9. To address CIP-007-3 R5.2.3 and R5.3.3, the UREs captured the Physical Security Servers' security access logs and reviews them weekly. In addition, the UREs changed the passwords for the shared accounts and will record such changes in the future in the change control management system;
10. To address CIP-007-3 R6.1 and R6.5, the UREs review security audit logs, for one of the identified systems, weekly; and
11. To address CIP-007-3 R8.2, the UREs included the Physical Security Servers in the annual cyber vulnerability assessment.

The UREs certified that the above Mitigation Plan requirements were completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that UREs' Mitigation Plan was completed.

**CIP-007-3 R2 (URE2: RFC201100790, URE1: RFC201100800, and URE3: RFC201100809)**

The UREs' Mitigation Plan to address the violations of CIP-007-3 R2 was submitted to Reliability*First* on November 15, 2011. The Mitigation Plan was accepted by Reliability*First* on January 6, 2012 and approved by NERC on February 6, 2012. The Mitigation Plan for the violations is designated as RFCMIT006669 and was submitted as non-public information to FERC on February 10, 2012 in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to:

1. Perform an annual cyber vulnerability assessment, during which they conducted a review of the required ports and services and compared the results to actual ports and services;
2. Enable only the required ports and services;

3. Continue to utilize the annual cyber vulnerability assessment process to determine which ports and services are required;
4. Address incremental changes to the ports and services through a change management process, which will ensure that only required ports and services are enabled; and
5. Ensure the change management process clearly describes the process for the analysis of the enabling and disabling ports and services.

The UREs certified that the above Mitigation Plan requirements for RFC201100800 and RFC201100790 were completed. The UREs certified that the above Mitigation Plan requirements for RFC201100809 were completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that UREs' Mitigation Plan was completed.

**CIP-007-3 R3 (URE2: RFC201100791, URE1: RFC201100801, and URE3: RFC201100810)**

The UREs' Mitigation Plan to address the violations of CIP-007-3 R3 was submitted to Reliability*First* on December 14, 2011. The Mitigation Plan was accepted by Reliability*First* on January 6, 2012 and approved by NERC on January 18, 2012. The Mitigation Plan for the violations is designated as RFCMIT006481 and was submitted as non-public information to FERC on January 20, 2012 in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to:

1. Enhance their security patch management procedures to clearly describe the mechanisms used to implement a thirty day tracking procedure for security patch releases;
2. Train relevant personnel to follow the new procedures;
3. Perform regular internal spot checks by the CIP compliance team to verify implementation of the new processes; and
4. Submit a Technical Feasibility Exception where applicable.

The UREs certified that the above Mitigation Plan requirements were completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that UREs' Mitigation Plan was completed.

**CIP-007-3 R8 (URE2: RFC201100794, URE1: RFC201100804, and URE3: RFC201100813)**

The UREs' Mitigation Plan to address the violations of CIP-007-3 R8 was submitted to Reliability*First* on November 15, 2011. The Mitigation Plan was accepted by Reliability*First* on January 6, 2012 and approved by NERC on February 6, 2012. The Mitigation Plan for the violations is designated as RFCMIT006670 and was submitted as non-public information to FERC on February 10, 2012 in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to add all networks within the ESP to the scope of the annual cyber vulnerability assessment, which included all Cyber Assets within the ESP.

The UREs certified that the above Mitigation Plan requirements were completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that UREs' Mitigation Plan was completed.

**Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed**[10]

**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,[11] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2012. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of an eighty thousand dollar ($80,000) financial penalty against the UREs 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

[10] *See* 18 C.F.R. § 39.7(d)(4).
[11] *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).

Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. the violations constituted the UREs' first occurrence of violations of the subject NERC Reliability Standards;
2. The UREs self-reported the violations;
3. Reliability*First* reported that the UREs were cooperative throughout the compliance enforcement process;
4. The UREs had a compliance program at the time of the violations which Reliability*First* considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. Reliability*First* determined that the violations posed a moderate risk but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. Reliability*First* reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of eighty thousand dollars ($80,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30 day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

**Request for Confidential Treatment**

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

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

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

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

**Attachments to be Included as Part of this Notice of Penalty**

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

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

   a. The UREs' Self-Report for CIP-005-3 R1, included as Attachment A to the Settlement Agreement;

   b. The UREs' Mitigation Plan for CIP-005-3 R1, included as Attachment B to the Settlement Agreement;

   c. The UREs' Self-Report for CIP-005-3 R2, included as Attachment C to the Settlement Agreement;

   d. The UREs' Mitigation Plan for CIP-005-2 R2, included as Attachment D to the Settlement Agreement;

   e. The UREs' Self-Report for CIP-005-2 R4, included as Attachment E to the Settlement Agreement;

   f. The UREs' Mitigation Plan for CIP-005-2 R4, included as Attachment F to the Settlement Agreement;

   g. The UREs' Self-Report for CIP-006-3 R2, included as Attachment G to the Settlement Agreement;

   h. The UREs' Mitigation Plan for CIP-006-3 R2, included as Attachment H to the Settlement Agreement;

   i. The UREs' Self-Report for CIP-007-3 R2, included as Attachment I to the Settlement Agreement;

   j. The UREs' Mitigation Plan for CIP-007-3 R2, included as Attachment J to the Settlement Agreement;

k. The UREs' Self-Report for CIP-007-3 R3, included as Attachment K to the Settlement Agreement;

l. The UREs' Mitigation Plan for CIP-007-3 R3, included as Attachment L to the Settlement Agreement;

m. The UREs' Self-Report for CIP-007-3 R8, included as Attachment M to the Settlement Agreement;

n. The UREs' Mitigation Plan for CIP-007-3 R8, included as Attachment N to the Settlement Agreement;

b) Record documents for the violation of CIP-005-3 R1, included as Attachment b:

1. The UREs' Certification of Mitigation Plan Completion; and
2. Reliability*First*'s Verification of Mitigation Plan Completion.

c) Record documents for the violation of CIP-005-3 R2, included as Attachment c:

1. The UREs' Certification of Mitigation Plan Completion for RFC201100786;
2. The UREs' Certification of Mitigation Plan Completion for RFC201100796;
3. The UREs' Certification of Mitigation Plan Completion for RFC201100806; and
4. Reliability*First*'s Verification of Mitigation Plan Completion.

d) Record documents for the violation of CIP-005-2 R4, included as Attachment d:

1. The UREs' Certification of Mitigation Plan Completion for RFC201100787;
2. The UREs' Certification of Mitigation Plan Completion for RFC201100797;
3. The UREs' Certification of Mitigation Plan Completion; and
4. Reliability*First*'s Verification of Mitigation Plan Completion.

e) Record documents for the violation of CIP-006-3 R2, included as Attachment e:

1. The UREs' Mitigation Plan for CIP-006-3 R2;
2. The UREs' Certification of Mitigation Plan Completion; and
3. Reliability*First*'s Verification of Mitigation Plan Completion.

f) Record documents for the violation of CIP-007-3 R2, included as Attachment f:

1. The UREs' Certification of Mitigation Plan Completion for RFC201100790;
2. The UREs' Certification of Mitigation Plan Completion for RFC201100800;
3. The UREs' Certification of Mitigation Plan Completion for RFC201100809; and
4. Reliability*First*'s Verification of Mitigation Plan Completion.

g) Record documents for the violation of CIP-007-3 R3, included as Attachment g:

1. The UREs' Certification of Mitigation Plan Completion; and
2. Reliability*First*'s Verification of Mitigation Plan Completion.

h) Record documents for the violation of CIP-007-3 R8, included as Attachment h:

1. The UREs' Certification of Mitigation Plan Completion for RFC201100794;
2. The UREs' Certification of Mitigation Plan Completion for RFC201100804;
3. The UREs' Certification of Mitigation Plan Completion; and
4. Reliability*First*'s Verification of Mitigation Plan Completion.

**A Form of Notice Suitable for Publication**[12]

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

[12] *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<br>(404) 446-2560<br><br>Charles A. Berardesco*<br>Senior Vice President and General Counsel<br>North American Electric Reliability Corporation<br>1325 G Street N.W., Suite 600<br>Washington, DC 20005<br>(202) 400-3000<br>(202) 644-8099 – facsimile<br>charles.berardesco@nerc.net<br><br>Robert K. Wargo*<br>Director of Analytics & 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 | Rebecca J. Michael*<br>Associate General Counsel for Corporate and Regulatory Matters<br>Sonia C. Mendonça*<br>Attorney<br>North American Electric Reliability Corporation<br>1325 G Street N.W.<br>Suite 600<br>Washington, DC 20005<br>(202) 400-3000<br>(202) 644-8099 – facsimile<br>rebecca.michael@nerc.net<br>sonia.mendonca@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 |

| | |
|---|---|
| | *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. |

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

**Conclusion**

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

Respectfully submitted,

*/s/ Rebecca J. Michael*

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Sonia C. Mendonça Attorney
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

cc: Unidentified Registered Entities
ReliabilityFirst Corporation

Attachments