November 25, 2014

**VIA ELECTRONIC FILING**

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. NP15-_-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's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the violations[3] addressed in this Notice of Penalty. The violations resolved by this Settlement Agreement concern URE's operations in ReliabilityFirst, Midwest Reliability Organization (MRO), and SERC Reliability Corporation (SERC), herein

[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 (2014). *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) and 18 C.F.R § 39.7(d).

[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.

referred to as the "Regions." Following extensive coordination and collaboration among the Regions, ReliabilityFirst entered into the agreement on behalf of itself, MRO, and SERC.

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed monetary penalty of seventy-five thousand dollars ($75,000), and an additional financial sanction in the form of a required investment of at least one hundred thousand dollars ($100,000) in support of additional reliability enhancements, 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. The violations in this Notice of Penalty 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. 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 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

| NERC Violation ID | Reliability Std. | Req. | VRF/VSL* | Total Penalty |
|---|---|---|---|---|
| RFC2013012304 | CIP-002-1 | R3 | High/High | $75,000 |
| RFC2012010916 | CIP-003-3 | R2 | Medium/Severe | |
| RFC2012010917 | CIP-003-3 | R3 | Lower/Severe | |
| RFC2012010328 | CIP-004-3 | R2 | Lower/Severe | |
| RFC2012010918 | CIP-005-1 | R1.5 | Medium/Severe | |
| RFC2012011084 | CIP-005-3a | R1.5 | Medium/Severe | |

| NERC Violation ID | Reliability Std. | Req. | VRF/VSL* | Total Penalty |
|---|---|---|---|---|
| RFC2012011370 | CIP-005-2 | R1.5 | Medium/Severe | $75,000 |
| RFC2013012307 | CIP-005-1 | R2 | Medium/Severe | |
| RFC2013012318 | CIP-005-1 | R4 | Medium/Severe | |
| RFC2013012319 | CIP-006-2 | R1 | Medium/Severe | |
| RFC2012011366 | CIP-006-2 | R2.2 | Medium/Severe | |
| RFC2012011373 | CIP-007-1 | R1 | Medium/Severe | |
| RFC2012011372 | CIP-007-2a | R2 | Medium/Severe | |
| RFC2012010919 | CIP-007-2a | R5 | Lower/Severe | |
| RFC2013012439 | CIP-007-2a | R6 | Lower/Severe | |
| RFC2012011371 | CIP-007-2a | R8 | Medium/Severe | |
| RFC2013012320 | CIP-008-1 | R1 | Lower/Severe | |
| RFC2013012321 | CIP-009-1 | R1 | Medium/Severe | |
| RFC2013012463 | CIP-009-1 | R5 | Lower/Severe | |

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

Background Information

This Settlement Agreement resolves 19 CIP violations discovered through a series of Self-Certifications, Self-Reports, and a multiregional Compliance Audit (Compliance Audit). ReliabilityFirst led the Compliance Audit on behalf of itself, MRO, and SERC.

CIP-002-1 R3 (RFC2013012304)[4]

During the Compliance Audit, ReliabilityFirst discovered a violation of CIP-002-1 R3. URE failed to document the review of two types of Cyber Assets to determine whether those assets were Critical Cyber Assets (CCAs). Specifically, URE failed to identify time and frequency devices and certain laptop computers as CCAs.

In addition, URE permitted remote access to certain laptop computers, which were not identified as CCAs. These laptop computers were essential to the operation of URE's Critical Assets.

ReliabilityFirst determined the duration of the violation to be from the date the standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's method of identifying CCAs relies on a top-down approach that first considers essential functions, identifies applications that support those functions, and then identifies Cyber Assets that support the applications. This method did not directly review Cyber Assets related to each CCA and could have resulted in a failure to identify CCAs. Further, the two assets at issue could have led to significant harm to the BPS.

Several factors mitigated the risk. With respect to the time and frequency devices, ReliabilityFirst determined that the likelihood of a bad actor accessing URE's data system and reaching the assets at issue was low due to the defense-in-depth security strategies URE employs, including the containment of these assets behind multiple layers of physical and electronic access controls, the application of URE's change management process to these assets, redundant configurations, and the application of account and access management controls such as strong, two-factor authentication.

With respect to the laptop computers, URE required employees to sign into and be physically present in URE's facilities to take any actions affecting the BPS. Therefore, the employees could not take BPS-related actions using the laptops at issue.

[4] ReliabilityFirst applied the version of the Reliability Standard in effect at the time each violation began.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its CCA identification process to ensure that all Cyber Assets related to each CCA are identified and reviewed; and
2. create a business process diagram that includes a quality control check. The diagram is designed to ensure that all CCAs are considered.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

<u>CIP-003-3 R2 and R3 (RFC2012010916 and RFC2012010917)</u>

URE submitted a Self-Report stating that it had issues with CIP-003-1 R2 and R3. URE failed to document the delegation of responsibilities by its senior manager to delegates. In four instances, a CIP cybersecurity manager signed extensions to cybersecurity exceptions without being formally designated as a delegate. In addition, on three instances, the cybersecurity exceptions were not reviewed annually by the senior manager.

ReliabilityFirst determined that URE had violations of CIP-003-1 R2 and R3 because the entity failed to document the delegation of responsibilities by its senior manager to delegates.

ReliabilityFirst determined the duration of the violation to be from the date URE failed to document the delegation of responsibilities to delegates, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The violation was documentation-related. Only one of the exceptions to the cybersecurity policy at issue was CIP-related. URE's mitigation strategy included appointing additional delegates, one of whom is the manager of cybersecurity. The manager of cybersecurity was qualified to review and approve the extensions, and was later designated to perform the task, as part of URE's mitigation.

URE's Mitigation Plan to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. obtain reviews and approvals by the appropriate CIP senior manager and document the appointment of delegates, including the manager of cybersecurity; and

2. conduct training on cybersecurity exceptions for the cybersecurity managers, their delegates, and for URE's cybersecurity department.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-004-3 R2 (RFC2012010328)

URE submitted a Self-Report stating that it had an issue with CIP-004 R2. As part of URE's annual review of its cybersecurity training program, URE attempted to update its program to incorporate information regarding cybersecurity threats. However, the training that URE finalized and adopted for use inadvertently omitted the information required by CIP-004-1 R2.2 regarding: i) the proper use of CCAs (R2.2.1); ii) electronic access controls to CCAs (R.2.2.2); and iii) recovery plans for CCAs after a Cyber Security Incident (R.2.2.4). URE used these training materials to provide training on two newly-hired employees and six newly-hired contractors.

In addition, during mitigation, URE identified an issue resulting from the conversion and re-formatting processes necessary to convert the training materials into the format utilized to train new employees.

ReliabilityFirst determined that URE had a violation of CIP-004-3 R2 because it failed to provide training that addressed all elements of this standard.

ReliabilityFirst determined the duration of the violation to be from the date URE failed to include all required information in its training materials, through when URE submitted revised evidence of mitigating activities to include the issue identified during its initial Mitigation Plan implementation.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All affected personnel had a personnel risk assessment and were eventually trained as required by the standard. The deficient cybersecurity training provided relevant information regarding preventing and defending against cybersecurity incidents, which was reinforced through URE's quarterly cybersecurity tips. The duration of the issue was limited due to the execution of URE's internal controls program.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. administer training to the individuals at issue; and

2. convert the cybersecurity training to a controlled document and conduct training on controls applicable to training revisions.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R1.5; CIP-005-3a R1.5; and CIP-005-2 R1.5 (RFC2012010918, RFC2012011084, and RFC2012011370)

URE submitted Self-Reports stating that it was in violation of CIP-005-1 R1.5. During the Compliance Audit, ReliabilityFirst discovered an additional instance of noncompliance with CIP-005-1 R1.5. In the course of mitigation, while implementing its improvement program, URE discovered an additional violation of this standard.

URE failed to: i) timely change passwords on 21 access control and monitoring devices (ACMs), CCAs, and non-CCAs; ii) locate two sets of ACMs in a Physical Security Perimeter (PSP) and afford the required protections; iii) afford the protections of CIP-007-1 R1 (test procedures) and R8 (cyber vulnerability assessment) to 52 ACMs; iv) consider electronic ACMs to be access points and afford the protections required by the standard; and v) identify additional access points to eight CCA servers.

ReliabilityFirst determined the duration of the first violation that was self-reported to be from the date the standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined the duration of the second violation that was self-reported to be from the date the devices were first commissioned into a facility not properly identified as a PSP, through when URE completed its Mitigation Plan.

ReliabilityFirst determined the duration of the third violation that was self-reported to be from the earliest date the devices at issue were commissioned, through the date the last two miscategorized devices were properly categorized and became subject to system administrator review.

ReliabilityFirst determined the duration of the violation discovered at the Compliance Audit and during mitigation to be from the date the standard became mandatory and enforceable, through when URE completed its improvement program.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to protect electronic security perimeter (ESP) access points and maintain secure passwords increases the likelihood of a gap in

security defenses for the ESP. The lengthy duration of the violations increased URE's exposure to this risk.

However, URE mitigated the risk by employing a defense-in-depth strategy that includes: i) a network operations center that actively monitors and responds to a host of enterprise-wide system performance and availability events. As a result, URE is capable of identifying any potentially disruptive network events before they impact BPS systems; ii) affording the assets at issue several protections, such as application of rigorous change management practices, consistent up-to-date patching, antivirus and malware prevention software, account and access management practices, and user and system logging and monitoring; and iii) locating the assets within controlled access facilities, which include protection against unauthorized physical access with multiple layers of electronic and physical access controls, such as guards, account management and access controls (e.g., strong, two-factor authentication). In addition, less than three percent of URE's non-user accounts had passwords that were overdue for change.

URE's Mitigation Plan to address the first self-reported violation was submitted to ReliabilityFirst. URE's Mitigation Plan required URE to:

1. change the passwords for all affected accounts; and
2. modify its process for creating new non-user accounts to require that accounts are monitored by its automated passwords management tool.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

URE's Mitigation Plan to address the second self-reported violation was submitted to ReliabilityFirst. URE's Mitigation Plan required URE to:

1. create documented PSPs for the facility that held the access control and monitoring devices;
2. validate that all protections associated with PSPs were present in the facility;
3. update employees' information; and
4. review its asset commissioning process to identify opportunities for improvement.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete. [5]

URE's Mitigation Plan to address the violation discovered at the Compliance Audit was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its cyber vulnerability assessment (CVA) and production readiness testing processes by defining criteria for justifications of firewall and access control list rule permissions; and
2. improve its processes to ensure that it conducts CVAs of non-critical Cyber Assets in, and electronic access points to, URE's ESPs and its ACMs.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R2 (RFC2013012307)

During the Compliance Audit, ReliabilityFirst discovered that URE violated CIP-005-1 R2. URE failed to demonstrate that it enables only ports and services required for operations. For example, for one device, URE failed to explain how various network objects were used, and failed to provide a business justification for open ports and services.

ReliabilityFirst determined that URE had a violation of CIP-005-1 R2 because URE failed to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to restrict access to protected networks leaves those networks open to attack, which may make protected systems vulnerable to unauthorized access. The duration of the violation increased URE's exposure to this risk.

[5] URE completed the mitigating activities associated with the third self-reported violation prior to submitting the Self-Report. URE established processes for cybersecurity testing associated with significant changes, and assigned the devices at issue to the correct domain. In addition, some of the devices were decommissioned or were no longer listed on URE's ESP workbook or active within the ESPs.

URE's defense-in-depth strategies, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370) mitigated the risk.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to improve its processes associated with defining criteria for justifications of firewall and access control permissions.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R4 (RFC2013012318)

During the Compliance Audit, ReliabilityFirst discovered a violation of CIP-005-1 R4 because URE failed to perform a comprehensive annual review of active ports and services.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE performed ongoing reviews on ports and services throughout the year as it made changes to its system. URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370), minimized the likelihood that an unauthorized person could access URE's data systems.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its processes associated with conducting CVAs of non-critical Cyber Assets and electronic access points to URE's ESPs and ACM devices; and
2. conduct a comprehensive annual review of all ports and services.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-006-2 R1 (RFC2013012319)

During the Compliance Audit, ReliabilityFirst discovered that URE had a violation of CIP-006-1 R1 because URE failed to contain all ESP Cyber Assets within a PSP.

Specifically, several PSPs at different locations had openings within the boundaries of the PSP that exceeded 96 square inches. Therefore, the PSPs did not provide a continuous six-wall boundary. In addition, the cabling between two rooms in one facility was not protected within a six-wall boundary. During the course of mitigation, URE discovered two additional PSP openings.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The openings at issue were obscured from observation because they were located above a dropped ceiling or below a raised floor. An individual attempting to exploit these unsecured openings would have required a special tool to access the openings.

In addition, the facility was staffed 24 hours a day, reducing the likelihood of unauthorized physical access. Access to any of the gaps would have been impeded by fire stop mechanisms, ductwork, wiring conduit, cable trays, or the steel infrastructure of the building. The location of the openings was within a restricted area with controlled access, camera surveillance, and other physical monitoring in place. The cabling between the two rooms in the facility had adequate defense-in-depth mechanisms and compensatory protective measures in place. URE's intrusion detection system and real-time monitoring of the Cyber Assets within the ESP remained intact throughout the duration of the violation.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. close all of the PSP openings;
2. revise the PSP plan to require confirmation that all the requirements for implementing a new PSP or commissioning a new building are addressed;
3. institute annual physical inspections to ensure there are no openings within the PSP;
4. submit a technical feasibility exception (TFE) request for the cabling between the two facilities, which ReliabilityFirst approved; and

5. install permanent mesh to close off the tunnel and permanently secure the hatches.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-006-2 R2.2 (RFC2012011366)

URE submitted a Self-Report stating it was in violation of CIP-006-2 R2.2. During mitigation, URE discovered and self-reported an additional instance of noncompliance.

URE failed to afford certain protective measures to the access points to the ESP. URE improperly categorized 75 Cyber Assets and failed to afford these devices the cybersecurity testing required by URE's procedures. Also, URE's physical access badge reader system controllers were not categorized as Cyber Assets that authorize and log access to a PSP.

ReliabilityFirst determined that URE had a violation of CIP-006-2 R2 because URE failed to afford access points to the ESP certain protective measures.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to conduct cybersecurity testing leaves Cyber Assets vulnerable to attacks. The duration of the violation increased URE's exposure to this risk. URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370), mitigated the risk. In addition, URE regularly monitored logs from the affected devices, and it did not experience any Cyber Security Incidents for the duration of the violation.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. move the devices at issue into the correct domain of its device-tracking system;
2. improve its processes associated with ensuring that all Cyber Assets within an ESP reside within an identified, complete PSP;
3. ensure that all assets that control and/or monitor access to physical security systems are afforded all protections required by CIP-006 R2.2.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R1 (RFC2012011373)

URE submitted a Self-Report stating it was in violation of CIP-007 R1. During the Compliance Audit, ReliabilityFirst discovered a second instance of noncompliance with CIP-007 R1. During mitigation, URE discovered two additional instances of noncompliance.

URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls. URE miscategorized 75 Cyber Assets and failed to afford these devices the cybersecurity testing required by URE's procedures and policy. In addition, URE: i) performed testing in its production environment rather than in an environment that reflects the production environment; ii) failed to perform cybersecurity testing for significant changes on certain turret servers;[6] and iii) failed to implement certain security patches.

ReliabilityFirst determined that URE had a violation of CIP-007-1 R1 for failing to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's practice of testing in the production environment raised the risk of adverse actions occurring in the production environment when system changes are implemented. The lengthy duration of the violation increased URE's exposure to the risk.

URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370) mitigated the risk. URE's change management process, which requires thorough functional testing of significant changes, also reduced the potential for unauthorized access.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. re-categorize many of the Cyber Assets or remove them from the ESP;

[6] URE's turret servers are vendor-managed appliances identified as CCAs that support phone operations.

2. improve its processes associated with cybersecurity testing; and
3. create internal controls for the generation and maintenance of its software lists.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-2a R2 (RFC2012011372)

URE submitted a Self-Report stating that it was in violation of CIP-007 R2. During the Compliance Audit, ReliabilityFirst discovered an additional noncompliance of this standard. Finally, during mitigation, URE discovered and self-reported a third instance of noncompliance.

URE failed to ensure that only ports and services required for normal and emergency operations were enabled. URE failed to: i) perform its processes and procedures for ports and services review on 75 Cyber Assets; ii) demonstrate that only ports and services required for normal and emergency operations were enabled for multiple systems; and iii) review weekly enterprise security manager scans.

ReliabilityFirst determined that URE had a violation of CIP-007-2a R2 because URE failed to maintain its process to ensure that only those ports and services required for normal and emergency operations are enabled.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to protect Cyber Assets within the ESP through a ports and services baseline increases the likelihood of a security gap. The lengthy duration of the violation increased URE's exposure to the risk.

URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370) mitigated the risk. URE's network configuration is such that traffic is limited based on specific protocols, which are required to be met to enter the network. The configuration prevents unsolicited traffic from passing into the networks segregated by ESPs, thereby reducing the risk to the BPS. Additional protections are provided by intrusion detection and prevention system devices that are programmed to detect for malicious traffic attempting to gain access to the ESP, regardless of whether the ports and services are enabled on the end-device. If the intrusion detection and prevention system detects malicious traffic, it prevents the malicious traffic from gaining access to

the network. URE consistently maintained up-to-date patching for all devices at issue, and the devices were protected by antivirus and malware prevention software.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. enhance its processes for ensuring the security of access to and through its electronic access points as well as the security of non-Critical Assets in URE's ESPs and ACMs; and
2. improve its processes to ensure that only those ports and services required for normal and emergency operations are enabled through URE's improvement program initiative for baseline configuration data and configuration management.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

<u>CIP-007-2a R5 (RFC2012010919)</u>

URE submitted a Self-Report stating that it was in violation of CIP-007 R5.3.3. URE discovered that 21 (3%) of the passwords for 706 non-user accounts for CCAs, ACM devices, and non-CCA Cyber Assets within the URE ESP were not changed annually.

During the Compliance Audit, ReliabilityFirst discovered that URE failed to create historical audit trails of individual user accounts access activity. Also, for an approved TFE, URE indicated that a mitigating process was in place to change account passwords every 180 days, but one device did not have the technical capabilities to enforce that process.

During mitigation, URE discovered and self-reported an additional instance of noncompliance. URE's information application is deemed to be a CCA. URE failed to review certain accounts associated with this application during its quarterly entitlement reviews. In addition, certain active directory groups used for access to PI were not accurately reflected in quarterly entitlement reviews.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The risk was mitigated because the account password issue was a documentation issue. Although URE failed to retain logs of sufficient detail to create historical audit trails of individual

user accounts, URE did produce, retain, and review logs of system security events. The logs at issue were for less than 10 % of the devices for which URE was logging and reviewing log activity. URE's network operations center actively monitors and responds to a host of enterprise-wide security tools and controls, which allows URE to identify any potentially disruptive network events and actual cybersecurity incidents before they impact systems related to the BPS.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

For a description of mitigating activities, see the Mitigation Plan for RFC2012010918, RFC2012011084, and RFC2012011370 described above.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

<u>CIP-007-2a R6 (RFC2013012439)</u>

URE submitted a Self-Certification stating that it was in violation of CIP-007 R6.

ReliabilityFirst determined that URE had a violation of CIP-007-2a R6 because URE failed to ensure that certain Cyber Assets within the ESP had automated tools or organizational process controls to monitor system events that are related to cybersecurity.

During mitigation, URE discovered that it had not filed TFEs for logging on certain vendor-managed devices. URE failed to review access logs for three turret servers, which are vendor-managed appliances initially identified as CCAs located in three facilities.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE conducted undocumented reviews of turret servers access logs at one of the facilities approximately monthly. URE also conducted undocumented reviews for alarming of the access logs for the turret servers in two facilities daily. In addition, the telephony controlled by the turret servers could have been replaced by other means of communication in the event of disruption. URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370), reduced the likelihood of an unauthorized actor accessing URE's data systems.

URE took the following mitigating actions:

1. review the turret servers' access logs for the previous 90 days and develop, document, and implement a process for the ongoing monthly review of turret server access logs, including documentation and retention of the review results;
2. initiate coordination with the turret servers' vendor to develop a formalized process for the performance of cybersecurity testing on the turret servers and to evaluate implementing an automated logging solution on the turret servers; and
3. replace the process and technology used for security status monitoring and logging.

ReliabilityFirst verified onsite that URE completed these mitigating actions.

CIP-007-2a R8 (RFC2012011371)

URE submitted a Self-Report stating that it was in violation of CIP-007 R8. During the Compliance Audit, ReliabilityFirst discovered an additional instance of noncompliance with this Standard.

URE failed to include the required elements in its CVA of 93 Cyber Assets within the ESP. URE failed to: i) have a CVA process that applies to all applicable devices within the scope of the requirement; ii) conduct annual review of the list of ports and services required for operation; iii) provide sufficient evidence of a review of the controls for default accounts; and iv) document results for all CVAs. Not all documented CVAs included action plans for remediation or execution status of the action plans.

ReliabilityFirst determined that URE had a violation of CIP-007-2a R8 because URE failed to include the required elements in its CVAs of Cyber Assets within the ESP.

ReliabilityFirst determined the duration of the violation to be from the earliest commissioning date of the devices at issue, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, the failure to define adequately and execute CVAs increases the likelihood of compromise to the assets subject to CVAs. The duration of the violation and the number of devices involved increased URE's exposure to the risk.

URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370), minimized the likelihood of an unauthorized actor assessing URE's data systems. URE observed no breaches or Cyber Security Incidents during the time period of this issue. With regard to ports and services, URE runs enterprise security scans on some systems on a weekly basis to ensure that the systems are operating in accordance with the baseline. With regard to controls, the enterprise

security scans are used to identify, among other things, configuration of default accounts although it does not review controls for default accounts.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its processes and procedures associated with CVAs to ensure that all applicable devices are subject to a CVA; and
2. document the results for all CVAs and develop action plans for remediation or execution status.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-008-1 R1 (RFC2013012320)

During the Compliance Audit, ReliabilityFirst discovered a violation of CIP-008 R1. ReliabilityFirst determined that, although URE has a Cyber Security Incident handling procedure, it did not include documented procedures to characterize and classify events as reportable Cyber Security Incidents.

ReliabilityFirst determined that URE had a violation of CIP-008-1 R1 because URE failed to include documented procedures to characterize and classify events as reportable Cyber Security Incidents in its Cyber Security Incident response plan.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the lack of specific procedures to handle reportable Cyber Security Incidents could result in a delayed response to a cyber attack. The lengthy duration of the violation increased URE's exposure to this risk.

URE mitigated the risk by having in place documented procedures addressing all other elements of CIP-008, and URE experienced no Cyber Security Incidents through the duration of the violation. URE's defense-in-depth strategies reduced the likelihood of a bad actor accessing URE's data systems.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. integrate an incident criteria decision tree into its Cyber Security Incident response plan; and
2. add criteria to characterize and classify events as reportable incidents.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-009-1 R1 (RFC2013012321)

During the Compliance Audit, ReliabilityFirst discovered a violation of CIP-009-1 R1. URE failed to create a recovery plan for CCAs. URE's yearly operational exercise, which used replicated backup (or "hot site"), was insufficient for disaster recovery of CCAs.

ReliabilityFirst determined that URE had a violation of CIP-009-1 R1 because URE failed to create a recovery plan for CCAs.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the use of a "hot site" leaves open the possibility that damage to Cyber Assets would be replicated to the only backup files, eliminating the possibility of restoration. The lengthy duration of the violation increased URE's exposure to the risk.

URE mitigated the risk by having mechanisms in place to protect CCAs against system events. URE not only backed up and stored the information required to restore CCAs, but was able to successfully restore various types of failed assets and data. Although URE's method of backup was insufficient for recovery purposes, it was sufficient for business continuity. URE's network operations center actively monitors and responds to a host of enterprise-wide system performance and availability events, which allows URE to identify any potentially disruptive network events before they impact systems related to the BPS. URE Cyber Assets were protected by firewalls, application of rigorous change management practices, consistent, up-to-date patching, antivirus and malware prevention software, account and access management practices, and user and system activity logging and monitoring. The assets were located within controlled access facilities, which provided protection against unauthorized physical access with multiple layers of electronic and physical access controls. URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370) also mitigated the risk.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its processes and procedures for recovering CCAs, backing-up and restoring those assets; and
2. ensure backup media required for restoring of these assets are properly tested.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-009-1 R5 (RFC2013012463)

During the Compliance Audit, ReliabilityFirst discovered a violation of CIP-009-1 R5. URE failed to test its backup media annually.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE afforded its Cyber Assets other protective measures to reduce the risk of failure and to minimize threats and vulnerabilities. Those protective measures included: locating the Cyber Assets behind access points, including firewalls; rigorous change management practices; implementing electronic and physical access controls to all Cyber Assets within the ESP and ESP access points; implementing antivirus software where technically feasible; and implementing user and system activity logging and monitoring of access points and Cyber Assets within the ESP. URE had backed up and stored the information required to successfully restore CCAs in the form of the tapes and, upon testing the network device backup media during typical and frequent restorations of activities, URE regularly confirmed that information was available. URE had implemented other mechanisms to maintain the information essential to recovery. Although URE's method of backup was insufficient for recovery purposes, it was sufficient for business continuity.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its processes and procedures for recovering CCAs and backing up and restoring those assets; and

2. ensure backup media required for restoring of these assets are properly tested.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a monetary penalty of seventy-five thousand dollars ($75,000) for the referenced violations. Further, as an additional financial sanction, URE shall provide evidence to demonstrate expenditures of at least one hundred thousand dollars ($100,000) in support of additional reliability enhancements. In reaching this determination, the Regions considered the following factors:

1. During the Compliance Audit, the Regions determined that all violations, when considered as a whole, represented a significant risk to the reliability of the BPS because they were a result of URE's weak cybersecurity compliance posture.
2. URE has prior violations of CIP-003, CIP-004, CIP-005, CIP-006, and CIP-007. ReliabilityFirst determined that the Compliance Audit was URE's first comprehensive CIP audit and many of the prior violations presented limited risk to the BPS. Therefore, the Regions did not consider URE's violation history as an aggravating factor in the penalty determination;
3. URE had an internal compliance program at the time of the violation, and the Regions considered certain elements of the program as a mitigating factor in the penalty determination;
4. URE undertook above-and-beyond compliance measures. URE began implementing its improvement program, which is a coordinated, broad effort to improve its cybersecurity stance and compliance with CIP standards.
5. URE agreed to perform reliability enhancements and outreach efforts.
6. The Regions negatively considered the duration of many of the violations. Because of the lengthy duration, URE allowed an elevated risk of exploitation of its Cyber Assets.
7. URE self-reported several of the violations;
8. URE was cooperative throughout the compliance enforcement process;
9. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
10. Eighteen of the violations posed a minimal or moderate risk to the reliability of the BPS. The violation of CIP-007-2a (RFC2012011371) posed a serious or substantial risk to the reliability of the BPS, as discussed above; and

11. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the monetary penalty amount of seventy-five thousand dollars ($75,000) and an additional financial sanction requiring expenditures of at least one hundred thousand dollars ($100,000) in support of additional reliability enhancements, is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

**Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed**[7]

**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,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on November 11, 2014 and approved 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 also considered the factors considered by the Regions, as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed monetary penalty of seventy-five thousand dollars ($75,000) and an additional financial sanction requiring the expenditure of at least one hundred thousand dollars ($100,000) 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.

---

[7] *See* 18 C.F.R. § 39.7(d)(4).

[8] *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).

**Request for Confidential Treatment**

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

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

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

**Attachments to be Included as Part of this Notice of Penalty**
REDACTED FROM THIS PUBLIC VERSION

**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>Vice President<br>Reliability Assurance & Monitoring<br>ReliabilityFirst Corporation<br>3 Summit Park Drive, Suite 600<br>Cleveland, OH 44131<br>(216) 503-0682<br>(216) 503-9207 facsimile<br>bob.wargo@rfirst.org | Sonia C. Mendonça*<br>Associate General Counsel and Senior Director of Enforcement<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>sonia.mendonca@nerc.net<br><br>Edwin G. Kichline*<br>Senior Counsel and Associate Director, Enforcement Processing<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>edwin.kichline@nerc.net<br><br>Niki Schaefer*<br>Managing Enforcement Attorney<br>ReliabilityFirst Corporation<br>3 Summit Park Drive, Suite 600<br>Cleveland, OH 44131<br>(216) 503-0689<br>(216) 503-9207 facsimile<br>niki.schaefer@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. | Jason Blake*<br>General Counsel & Corporate Secretary<br>ReliabilityFirst Corporation<br>3 Summit Park Drive, Suite 600<br>Cleveland, OH 44131<br>(216) 503-0683<br>(216) 503-9207 facsimile<br>jason.blake@rfirst.org<br><br>Kristina Pacovsky*<br>Counsel<br>ReliabilityFirst Corporation<br>3 Summit Park Drive, Suite 600<br>Cleveland, OH 44131<br>(216) 503-0670<br>(216) 503-9207 facsimile<br>kristina.pacovksy@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/ Edwin G. Kichline*
Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@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
(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

Sonia C. Mendonça
Associate General Counsel and Senior
Director of Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Reliability First Corporation, Midwest Reliability Organization, SERC Reliability Corporation

Attachments