PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

April 30, 2015

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 Entities
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 1 (URE1), Unidentified Registered Entity 2 (URE2), Unidentified Registered Entity 3 (URE3), Unidentified Registered Entity 4 (URE4), and Unidentified Registered Entity 5 (URE5), (collectively the UREs), NERC Registry ID#s NCRXXXXX, NCRXXXXX, NCRXXXXX, NCRXXXXX, and 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 resolves two sets of violations discovered through Self-Reports and Compliance Audit findings. The violations of the Unidentified Registered Entities are the remaining open enforcement actions from a CIP Compliance Audit that the UREs contested, but ultimately agreed to mitigate. The remaining violations are Self-Reports and Compliance Audit findings, many of which are minimal risk, documentation issues that would have been eligible for Compliance Exception treatment but for UREs' relevant compliance history.

[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).

The resolution of these violations are close in proximity to the FERC-approved settlement of 35 prior violations of the four UREs subject to this Settlement Agreement and other entities. While entering into the prior Settlement Agreement, ReliabilityFirst was aware of the extent and nature of the CIP compliance audit findings, and noted in the prior Settlement Agreement that the findings which are the subject of the instant Settlement Agreement demonstrated that UREs had made significant progress in terms of compliance. Although ReliabilityFirst was not in a position to resolve the instant Alleged Violations at that time of resolving the prior Settlement Agreement, given their isolated, mostly minimal risk nature, and the fact that they actually demonstrate a marked improvement in the UREs over time, ReliabilityFirst determined that a monetary penalty was neither necessary nor appropriate. The UREs were sanctioned fully for the shortcomings of their prior legacy CIP compliance program in the prior Settlement Agreement.

This Notice of Penalty is being filed with the Commission because ReliabilityFirst and UREs 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. According to the Settlement Agreement, the UREs neither admit nor deny the violations, but have agreed to the assessed penalty of zero dollars ($0), 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 in this Full 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 (2015), NERC provides the following

[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.

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*	Applicable Function(s)	Total Penalty
RFC2012011266	CIP-002-1	R3.1	Lower/Severe	URE3; URE4; URE5	$0
RFC2012011263	CIP-002-1	R3.1	High/Severe	URE3; URE4; URE5	
RFC2012011269	CIP-002-1	R3.1	Lower/Severe	URE3; URE4; URE5	
RFC2013012717	CIP-003-3	R6	Lower/Severe	URE1	
RFC2013012401	CIP-004-3	R4	Lower/ Lower	URE1	
RFC2013012512	CIP-005-1	R1.5	Medium/ Severe	URE1	
RFC2013012402	CIP-005-3	R5	Lower/ Severe	URE1	
RFC2013013005	CIP-006-1	R1.1	Medium/ Severe	URE1; URE2	
RFC2013013006	CIP-006-1	R1.1	Medium/ Severe	URE1; URE2	
RFC2013012303	CIP-006-3c	R1.1	Medium/ Severe	URE1	
RFC2013013007	CIP-006-1	R1.8	Medium/ Severe	URE1	

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Applicable Function(s)	Total Penalty
RFC2013012409	CIP-006-3c	R4	Medium/ Severe	URE1	$0
RFC2013012410	CIP-007-1	R2	Medium/ Severe	URE1; URE2	
RFC2013012413	CIP-007-1	R2	Medium/ Severe	URE1; URE2	
RFC2013012513	CIP-007-1	R3	Lower/ Severe	URE1; URE2	
RFC2013012514	CIP-007-1	R3	Lower/ Severe	URE1; URE2	
RFC2013012411	CIP-007-1	R5.2.1	Medium/ High	URE1	
RFC2013012412	CIP-007-1	R5.3.3	Medium/ Severe	URE1; URE2	
RFC2013012414	CIP-007-1	R5.3.3	Medium/ Severe	URE1; URE2	
RFC2013012753	CIP-007-3a	R1	Medium/ Severe	URE1; URE2	
RFC2013012768	CIP-007-3a	R1	Medium/ Severe	URE1; URE2	
RFC2013012718	CIP-007-3a	R6	Lower/ Severe	URE1	

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

CIP-002-1 R3.1 (RFC2012011263, RFC2012011266, RFC2012011269)

These violations include previously unresolved, contested issues from two CIP Compliance Audits of certain URE registrations.

ReliabilityFirst conducted a Compliance Audit of URE3, URE4, and URE5. This Agreement resolves three remaining violations of CIP-002-1 R3.1 that were not resolved by the prior Settlement Agreement.

During the Compliance Audit, ReliabilityFirst discovered that URE Companies were in violation of CIP-002-1 R3.1. ReliabilityFirst discovered an electronic access control and monitoring device (EACM) that allowed Cyber Assets, specifically remote terminal units (RTUs), to connect to the EACM and communicate using a routable protocol. URE3, URE4, and URE5 failed to identify these assets as Critical Cyber Assets (CCAs).

ReliabilityFirst determined that URE3, URE4, and URE5 had violations of CIP-002-1 R3.1 because they failed to identify certain Cyber Assets essential to the operation of a Critical Asset as CCAs. The Cyber Assets, in this case the RTUs, communicated outside an Electronic Security Perimeter (ESP) using a routable protocol.

ReliabilityFirst determined the duration of the violations to be from the date URE3, URE4, and URE5 were required to comply with the Reliability Standard through when the Mitigation Plans associated with these violations are scheduled for completion.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). Although URE3, URE4, and URE5 did not identify the RTUs as CCAs, they did provide most of the protections required for CCAs, thereby reducing risk to those devices. For example, the RTUs were afforded the protections of CIP-006 and the physical access protections of CIP-004 using an advanced secure access management tool with two-factor authentication in most cases, and rigorous change control, including patching.

URE3, URE4, and URE5's Mitigation Plans to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required URE3, URE4, and URE5 to:

1. develop a new Cyber Systems Identification Methodology for Bulk Electric System (BES) assets as part of the transition to CIP Version 5 compliance, , which will require the identification of serially connected Cyber Assets associated with substations as Medium Impact BES Cyber Assets without external routable connectivity; and

2. ensure that the RTUs meet the applicable minimum requirements for Medium BES Cyber Systems.

CIP-003-3 R6 (RFC2013012717)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-003-3 R6. URE1 reported that it did not follow its change control process in one instance due to human error. URE1's change control process requires changes to be logged and approved by a member of its change management advisory committee (Committee) prior to work being executed.

Although a change was verbally approved by the supervisor of the change owner and the business unit, it was not approved by a Committee member as required. URE1 discovered the violation while reviewing change requests older than 30 days that had not been closed.

ReliabilityFirst determined that URE1 violated CIP-003-3 R6 because it failed to establish and document a process of change control and configuration management for adding, modifying, replacing, or removing CCA hardware or software, and failed to implement supporting configuration management activities to identify, control, and document all entity or vendor-related changes to hardware and software components of CCAs, pursuant to its change control process.

ReliabilityFirst determined the duration of the violation to be from the date URE1 was required to comply with this Reliability Standard, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although the change control process was not followed appropriately, the change was approved by knowledgeable URE1 staff prior to the start of the work. In addition, URE1 timely performed mitigating actions to prevent recurrence of the error.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. require all personnel to validate that all changes are approved and documented prior to the start of work;
2. emphasize the approval process and requirements with responsible teams during meetings in the calendar year; and
3. review the process again via email reminder in the calendar year.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-004-3 R4 (RFC2013012401)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-004-3 R4. URE1 reported that during a review of local users on four Physical Access Control System (PACS) servers on its corporate network, it noticed that access to the PACS was not authorized and documented through URE1's access database for certain information technology employees and contractors. Due to human error, access authorizations were not properly established for these servers. Upon discovery, URE1 removed access for the affected individuals.

ReliabilityFirst determined that URE1 violated CIP-004-3 R4 because it failed to maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to CCAs, including the personnel's specific electronic and physical access rights to CCAs.

ReliabilityFirst determined the duration of the violation to be from the date URE1 was required to comply with CIP-004-3 R4, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although the devices were not set up to ensure individuals were granted proper access through the access system, those individuals had completed CIP training and were subject to personnel risk assessment (PRAs). In addition, access was granted through an approval process with the correct asset owners, just not through the proper access database. URE1 demonstrated an otherwise strong access control program, as evidenced by a subsequent Compliance Audit identifying no additional CIP-004 issues.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. remove access for the individuals;
2. define and authorize access through the proper access database; and
3. conduct a training to communicate the new access database account configuration to relevant employees.

URE1 certified that the above Mitigation Plan requirements were completed.

CIP-005-1 R1.5 (RFC2013012512)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-005-1 R1.5. URE1 reported that it did not identify and document one EACM device on CIP Cyber Asset lists. Consequently, this device was not afforded all of the protections listed in CIP-005 R1.5.

URE1 conducted a root cause analysis and determined that because the EACM is not located at the Critical Asset it supports, previous routine inspections did not account for the EACM, which is located several miles from the associated Critical Asset substation. The EACM is connected via non-routable microwave transport to the substation, and this non-hard-wired connection was overlooked.

ReliabilityFirst determined that URE1 violated CIP-005-1 R1.5 because it failed to ensure that one EACM was afforded the protective measures listed in CIP-005-1 R1.5.

ReliabilityFirst determined the duration of the violation to be from the date URE1 was required to comply with CIP-005-1 R1.5, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. First, although the EACM is an access point to an ESP, the EACM carries non-essential data to a substation containing no CCAs. Second, the type of connectivity used by the EACM is unique within the URE1 environment, and therefore is an isolated issue. Finally, the problem was detected by URE1 and promptly mitigated upon discovery.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. bring the EACM into compliance with CIP-005 R1.5, including implementing a Physical Security Perimeter (PSP) at the associated substation; and
2. validate all electronic configurations and update documentation to reflect these changes.

URE1 certified that the above Mitigation Plan requirements were completed.

CIP-005-3 R5 (RFC2013012402)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-005-2 R5. URE1 reported that a new drawing became the official, active energy management system (EMS) ESP diagram, superseding a previous drawing. Subsequent to that change, four approved changes were

made to various devices related to this environment. However, the applicable ESP diagram was not updated appropriately during the 90-day requirement period.

ReliabilityFirst determined that URE1 violated CIP-005-3 R5 because they failed to update documentation within the 90-day requirement period.

ReliabilityFirst determined the duration of the violation to be from the date URE1 failed to update documentation of the ESP within 90 days of the first change, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. ReliabilityFirst determined that the issue relates solely to documentation of the changes on the ESP diagram, and appears to be an isolated incident based on the fact that no other violations of CIP-005 R5 were identified during a subsequent Compliance Audit.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. update its ESP diagram and its procedure governing how information technology CIP Cyber Asset information and lists are maintained for annual reviews and ongoing changes. URE1 placed special emphasis on the thorough verification of devices depicted on ESP diagrams;
2. validate all access points to the ESP; and
3. appropriately reflect that information with the Cyber Asset lists.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1.1 (RFC2013013005 and RFC2013013006)

During the Compliance Audit, ReliabilityFirst discovered that URE1 and URE2 were in violation of CIP-006-1 R1.1.

For URE1, one facility drawing did not properly reflect the PSP, and the wiring between two PSPs was not completely enclosed by a six-wall border. For URE2, the wiring between two sets of PSPs was not contained within six-wall borders, and two rooms containing Cyber Assets were not declared as PSPs.

ReliabilityFirst determined that URE1 and URE2 violated CIP-006-1 R1.1 because they failed to ensure and document that all Cyber Assets within an ESP reside within an identified PSP.

ReliabilityFirst determined the duration of the violations to be from the date URE1 and URE2 were required to comply with CIP-006-1 R1.1, through the date URE1 and URE2 completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the physical locations affected by the violations were within corporate security boundaries and therefore less likely to be subject to harm by an external malicious actor. Second, each occurrence was an isolated incident and was mitigated promptly upon discovery by URE1's and URE2's fast and thorough response. These were minor wiring, documentation, and declaration issues that were mitigated promptly before the end of the onsite audit

Prior to the conclusion of the Compliance Audit, URE1 and URE2 modified drawings, enclosed cabling in conduit, filed Technical Feasibility Exceptions (TFEs), and established PSPs where needed. ReliabilityFirst verified these mitigating activities during the Compliance Audit. In addition, URE1 and URE2 also submitted formal Mitigation Plans.

URE1's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

URE2's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. revise the facility drawing to show that one PSP encompassed the entire floor; and
2. file a TFE to mitigate the wiring issue between the two PSPs.

URE2's Mitigation Plan required URE2 to:

1. file a TFE to mitigate the wiring issue between the two rooms containing Cyber Assets;
2. install conduit around the wiring between the two PSPs; and
3. enhance the PSP drawings to show how ESP wiring between multiple PSPs is provided physical protections.

URE1 and URE2 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's and URE2's Mitigation Plans were complete.

CIP-006-3c R1.1 (RFC2013012303)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-006-3c R1.1. URE1 reported that during an inspection of a PSP during remodeling activities, URE1 discovered openings greater than 96 square inches; openings in an overhead wall, openings in PSP walls, and an opening beneath a raised floor. These non-compliant openings were not discovered previously by routine inspections conducted by an independent contractor.

ReliabilityFirst determined that URE1 violated CIP-006-3c R1.1 because it failed to document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) addressing, at a minimum, that all Cyber Assets within an ESP shall reside within an identified PSP.

ReliabilityFirst determined the duration of the violation to be from the date URE1 created the openings in the PSP, the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Access to the PSP associated with the non-compliant openings was monitored continuously by security. Additionally, of the openings discovered, an opening under the raised floor abutted against a hallway within a secured non-CIP area. Some were overhead openings that were above dropped ceilings, which resulted in very limited visibility, and could have only been accessed with a ladder. The remaining openings were in PSP walls. The wall openings were created by remodeling activities and the other wall opening abutted against a secured hallway that allowed only individuals authorized to be in the facility to enter. URE1 mitigated the issue promptly upon discovery. The discovery was a result from an internal control related to physical security.

URE1's Mitigation Plan to address this violation was submitted to ReliabilityFirst as complete.

URE1's Mitigation Plan required URE1 to:

1. perform an extent of condition review and secure all openings with steel mesh; and
2. revise its physical security plan to inspect new physical security perimeters to prevent similar violations.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1.8 (RFC2013013007)

During the Compliance Audit, ReliabilityFirst discovered that URE1 was in violation of CIP-006-1 R2.2. URE1 used two terminal servers as workstations for its PACS, but did not identify those terminal servers as a PACS system, therefore failing to provide some of the protections identified in CIP-006 R2.

ReliabilityFirst determined that URE1 violated CIP-006-1 R1.8 because it failed to document and implement the operational and procedural controls to manage physical access at two access points to the PSPs twenty-four hours a day, seven days a week with one or more physical access methods.

ReliabilityFirst determined the duration of the violation to be from the date URE1 was required to comply with CIP-006-1 R1.8, through the date URE1 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 terminal servers cannot be used to authorize or log access directly to PSPs. The terminal servers themselves are located in PSPs and were afforded most of the protections required by CIP-006 R1.8. In addition, prior to the Compliance Audit, URE1did not realize these terminal servers could be considered part of the PACS system and should therefore be subject to the protections listed in CIP-006 R1.8. Thus, the violation did not result from a failure to institute internal controls for physical security.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst. The Mitigation Plan required URE1 to ensure the two terminal servers meet all CIP Standard requirements.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-006-3c R4 (RFC2013012409)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-006-3c R4. URE1 reported that an employee without authorized unescorted access to a substation accessed the substation without a valid key card. When the entry was made, URE1's security alarms station received an alarm, security technicians immediately investigated and escorted the employee out of the substation.

A physical security technician determined that the door lock had been disabled for the substation door and the actuation of a push button lever inside the door locking mechanism allowed the employee to

enter the substation. Although URE1 cannot conclusively determine the duration of the condition, it believes the period to be less than five days. A locksmith permanently disabled the levers in the substation door-locking mechanisms.

ReliabilityFirst determined that URE1 violated CIP-006-3c R4 because it failed to document and implement the operational and procedural controls to manage physical access at all access points to the PSP twenty-four hours a day, seven days a week with one or more physical access methods.

ReliabilityFirst determined the duration of the violation to be from the earliest date that URE1 believes it did not manage the physical access point, through the date URE1 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 door was adequately monitored during the period the lock was mechanically disabled. Only one unauthorized entry occurred during this period. The unauthorized individual was an employee with a current PRA. His entry to the substation was observed by authorized employees. The entry also resulted in an alarm, and security personnel ensured the individual was escorted out of the substation within ten minutes of his entry. In addition, the substation is located within a protected area that is continuously staffed with security officers.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. contract a locksmith to replace the locking mechanism with a proper lock;
2. perform an evaluation to determine if any additional inadequate lock mechanisms were installed at other substation PSPs; and
3. replace three additional inadequate locking mechanisms, which were identified through the extent-of-condition evaluation.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

<u>CIP-007-1 R2 (RFC2013012410 and RFC2013012413)</u>

URE1 and URE2 submitted Self-Reports to ReliabilityFirst stating that they were in violation of CIP-007-1 R2. URE1 and URE2 reported that their Cyber Vulnerability Assessments (CVAs) were the first under the new CIP compliance program.

The CVAs used a new procedure that provides better visibility to ports and services and demonstrated that existing documentation of ports and services was inadequate. URE1 identified Cyber Assets for which ports and services not needed for normal or emergency operations were not disabled, and Cyber Assets for which ports or services were not documented correctly. URE2 identified Cyber Assets for which ports and services not needed for normal or emergency operations were not disabled, and Cyber Assets for which ports or services were not documented correctly.

ReliabilityFirst determined that URE1 and URE2 violated CIP-007-1 R2 by failing to implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

ReliabilityFirst determined the duration of the violations to be from the date URE1 and URE2 were required to comply with CIP-007-1 R2, through the date URE1 and URE2 completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a moderate and not serious or substantial risk to the reliability of the BPS. A significant number of Cyber Assets suffered the deficiency, which potentially created vulnerabilities on those Cyber Assets for an extended period. Layers of defense on the UREs' network, such as intrusion prevention, limit the risk and exposure of devices to external threats. URE had robust intrusion prevention appliances on the internet-facing side of its environment and has intrusion prevention services on its firewalls in front of its EMS/GMS ESPs. URE1 and URE2 mitigated these violations by self-identifying the issues through improvements to its post-merger compliance program and performing thorough mitigation.

URE1's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

URE2's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

The Mitigation Plans required URE1 and URE2 to:

1. perform an evaluation of the ports and services program and procedures;
2. revise the associated procedures to improve the effectiveness, efficiency, and documentation of the CIP-007 R2 configuration program and shift the performance of CIP-007 R2 activities to asset owners and administrators; and
3. add new controls that track all changes made to the documentation. The controls relate back to the ticket that was generated in the change control and configuration management system.

URE1 and URE2 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

ReliabilityFirst verified that URE2's Mitigation Plan was complete.

CIP-007-1 R3 (RFC2013012513 and RFC2013012514)

URE1 and URE2 submitted identical Self-Reports to ReliabilityFirst stating that they were in violation of CIP-007-1 R3. URE1 and URE2 reported that during a system account review of the CIP environment they did not meet the 30-day self-imposed time limit in their security patch management program for documenting a patching implementation plan on two CCAs (servers).

Soon after the discovery of the violations, URE1 and URE2 developed an implementation plan to retire the two servers and migrate associated guest servers to physical servers, with all patches applied.

ReliabilityFirst determined that URE1 and URE2 violated CIP-007-1 R3 because they failed to provide sufficient evidence that their security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for Cyber Assets within the ESP was implemented for two applicable assets.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE1 and URE2, through the date URE1 and URE2 completed their respective Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the violations affected only two devices and were caused by an isolated human error, and there were no indications of a systemic failure in assessing or implementing security patches. Second, although the self-imposed 30-day time limit for patch implementation plan documentation was not met, applicable security patches and security upgrades were assessed for applicability within 30 calendar days as specifically required by the Standard. Finally, the subsequent Compliance Audit revealed no further violations of CIP-007 R3.

URE1's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

URE2's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

The Mitigation Plans required URE1 and URE2 to:

1. develop and review an implementation plan and retire the Cyber Assets affected; and

2. develop an internal control mechanism to monitor whether business units and/or system administrators document patch implementation plans within 30 days from the date of notification by their internal cyber security department.

URE1 and URE2 certified that the above Mitigation Plans' requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

ReliabilityFirst verified that URE2's Mitigation Plan was complete.

CIP-007-1 R5.2.1 (RFC2013012411)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-007-1 R5.2.1. URE1 reported that due to misleading documentation, URE1 failed to rename several EACM accounts as required by CIP-007 R5.2.1. In addition, URE1 reported that it failed to rename one other local default administrator account. These issues were discovered when a new tool for password change review was implemented. The violation affected Cyber Assets.

ReliabilityFirst determined that URE1 violated CIP-007-1 R5.2.1 because they failed to implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges, including factory default accounts, including the removal, disabling, or renaming of such accounts where possible.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE1, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the risk was mitigated partially by the Cyber Assets' location behind firewalls in an ESP; separate user accounts are required to log into the network, which were subject to multiple password change cycles. Second, although the accounts were not renamed for a long period and several cycles of CVAs did not identify the issue, URE1 has since significantly improved these internal controls, which enabled it to identify and self-report the issue.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. develop and implement a plan utilizing URE1's Change Management Process to rename the local administrator account on all affected devices;

2. rename the single account and a new step was added to the CIP server build process;
3. develop an improved CVA program that is capable of promptly identifying these types of deficiencies; and
4. perform an annual review of CIP Cyber Asset passwords and accounts. As part of these reviews, administrator, shared, and other generic accounts are reviewed to ensure they are still valid and required.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-007-1 R5.3.3 (RFC2013012412 and RFC2013012414)

URE1 and URE2 submitted Self-Reports to ReliabilityFirst stating that they were in violation of CIP-007-1 R5.3.3. URE1 reported that the passwords on local server accounts were not changed annually, and URE2 reported that the passwords on additional local server accounts were not changed annually. In both cases, although URE1 and URE2 have a procedure for annual local administrator account password updates, they missed the affected accounts because they were not documented in the password vault used to manually manage passwords. These password deficiencies were identified shortly after URE1 and URE2 implemented a new tool for password change reviews.

ReliabilityFirst determined that URE1 and URE2 violated CIP-007-1 R5.3.3 because they failed to require and use passwords that are changed at least annually.

ReliabilityFirst determined the duration of the violations to be from the date URE1 was required to comply with CIP-007-1 R5.3.3, through the date URE1 and URE2 completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the affected Cyber Assets are located behind firewalls in an ESP, and separate user accounts are required to log into the network, which were subject to multiple password change cycles through the duration of the violation. Second, although the passwords were not changed for a long period and several cycles of CVAs did not identify the issue, URE1 and URE2 have since significantly improved these internal controls, which enabled them to identify and self-report the issue.

URE1's Mitigation Plan to address its violation was submitted as complete to ReliabilityFirst. URE2's Mitigation Plan to address its violation was submitted as complete to ReliabilityFirst.

The Mitigation Plans required URE1 and URE2 to:

1. create a report that validates password changes and documents the use of the report in the associated procedure; and
2. add a new step to the CIP server build process to perform a peer review of the local server accounts for the new server and verify that the accounts and passwords are documented.

URE1 certified that the above Mitigation Plan requirements were completed. UER2 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

ReliabilityFirst verified that URE2's Mitigation Plan was complete.

CIP-007-3a R1 (RFC2013012753 and RFC2013012768)

URE1 and URE2 each submitted Self-Reports to ReliabilityFirst stating that they were in violation of CIP-007-3a R1. URE1 and URE2 did not maintain complete documentation of test results for significant changes on CIP Cyber Assets. URE1 did not document significant changes on Cyber Assets, and URE2 did not document significant changes on additional Cyber Assets.

ReliabilityFirst determined that URE1 and URE2 violated CIP-007-3a R1 because they failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls and failed to document test results.

ReliabilityFirst determined the duration of the violations to be from the date URE2 first failed to comply with CIP-007-3a R1, through the date URE1 and URE2 completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the violations were primarily a documentation issue, since URE1 and URE2 performed appropriate testing. Second, although not complete enough to meet the threshold of compliance, URE1 and URE2 did document some testing. Finally, URE1's and URE2's follow-up testing verified there were no adverse effects on the production system from the testing documentation inadequacies.

URE1's Mitigation Plan to address its violation was submitted as complete to ReliabilityFirst. URE2's Mitigation Plan to address its violation was submitted as complete to ReliabilityFirst.

URE1's and URE2's Mitigation Plans required URE1 and URE2 to:

1. have follow-up testing to verify that no adverse effects on the production systems or the operation of the production systems resulted from the testing documentation inadequacies;
2. meet with personnel to review and reinforce requirements and expectations for documenting test results for significant changes to CIP Cyber Assets; and
3. provide refresher training sessions to review and reinforce requirements and expectations of test results documentation for appropriate personnel.

URE1 and URE2 certified that the above Mitigation Plans' requirements were completed.

ReliabilityFirst verified that the Mitigation Plans were complete.

CIP-007-3a R6 (RFC2013012718)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-007-3a R6. URE1 reported that logs of system events over a 25-day period for one CCA were not retained for the full 90 days, as required by CIP 007-3a R6.

ReliabilityFirst determined that URE1 violated CIP-007-3a R6 because it failed to ensure that a Cyber Asset within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

ReliabilityFirst determined the duration of the violation to be from the date the CCA was initially misconfigured, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although the log entries were missing for one CCA device, this CCA device exists within the ESP, behind firewalls. The process and procedures were in place to monitor and log access at access points in the ESP. However, the violation was discovered by an effective internal control (quarterly review) and was limited to one device for a 25-day period before URE1 correctly configured it. In addition, no additional violations of CIP-007 R6 were discovered at the subsequent Compliance Audit.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. update a CIP server build procedure to emphasize the step for configuring the CCA to back up logs and automate alerting for potential cyber security failed login attempts;
2. add a CIP server build procedure for the peer review process; and
3. add a procedure step to include additional signoffs confirming that a test of the log backup configuration and automated alerting was successful.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed no monetary penalty for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors:

1. The UREs had prior violations of the subject NERC Reliability Standards. ReliabilityFirst did not consider these prior violations as aggravating factors in the penalty determination because the prior instances were isolated incidents that did not indicate repetitive conduct or systemic issues;
2. The UREs had an internal compliance program at the time of the violations which ReliabilityFirst considered a mitigating factor;
3. ReliabilityFirst determined that the UREs had made significant progress in terms of compliance since the Compliance Audit, which was considered a mitigating factor in the penalty determination.
4. The UREs self-reported 11 of the violations;
5. The UREs were cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. The violations of RFC2013012410 and RFC2013012413 posed a moderate but did not pose a serious or substantial risk to the reliability of the BPS while the rest of the violations posed a minimal risk, as discussed above; and
8. 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 no penalty 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[4]

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,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on April 13, 2015 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.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that no penalty 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.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *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).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer 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* Deputy General Counsel and Vice President of Compliance and 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 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

Kristina Pacovsky* Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0670 (216) 503-9207 facsimile kristina.pacovksy@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.	Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0682 (216) 503-9207 facsimile bob.wargo@rfirst.org Niki Schaefer* Managing Enforcement Attorney ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0689 (216) 503-9207 facsimile niki.schaefer@rfirst.org Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0683 (216) 503-9207 facsimile jason.blake@rfirst.org

Conclusion

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

Respectfully submitted,

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

/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

Sonia C. Mendonça
Deputy General Counsel and Vice President
of Compliance and 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 Entities
ReliabilityFirst

Attachments