NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

February 29, 2016

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. NP16-_-000

Dear Ms. Bose:

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[1] 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 violations of NERC CIP Reliability Standards.

According to the Settlement Agreement, URE stipulates to the facts included in the Settlement Agreement and admits that these facts may constitute violations. URE has agreed to the assessed penalty of one million seven hundred thousand dollars ($1,700,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement by and between ReliabilityFirst and URE. 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

[1] 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.

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 summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	Discovery Method* Date	Risk	Penalty Amount
RFC2014014245	CIP-002-3	R3	CA	Moderate	$1,700,000
RFC2014014014	CIP-003-1	R6	SR	Serious	
RFC2014014251	CIP-004-3	R2	CA	Moderate	
RFC2014014252	CIP-004-3	R2.1		Serious	
RFC2014014253	CIP-004-3	R3.3		Moderate	
RFC2013013197	CIP-004-3a	R4.2	SR		
RFC2014013447	CIP-004-3a	R4.2	SR		
RFC2014013997	CIP-004-3a	R4.2	SR		
RFC2014013623	CIP-005-1	R1.5	SR	Serious	
RFC2014014015	CIP-005-3a	R1.5	SR	Minimal	
RFC2014014207	CIP-005-3	R1.6	CA	Serious	
RFC2015015300	CIP-005-3a	R1			
RFC2014014410	CIP-006-3c	R1	SR	Minimal	
RFC2014014011	CIP-006-1	R1.1	SR	Moderate	

NERC Violation ID	Standard	Req	Discovery Method* Date	Risk	Penalty Amount
RFC2014014208	CIP-006-3a	R1.8	CA	Moderate	$1,700,000
RFC2015015143	CIP-006-3a	R1	SR		
RFC2014014209	CIP-006-3a	R5	CA	Serious	
RFC2013013198	CIP-006-3c	R5	SR		
RFC2014014211	CIP-007-3a	R1.3	CA		
RFC2014013998	CIP-007-1	R2	SR		
RFC2014013626	CIP-007-1	R3	SR		
RFC2014014262	CIP-007-3a	R3, R3.1, R3.2	SR		
RFC2014014114	CIP-007-3a	R3.2			
RFC2014014012	CIP-007-3a	R4	SR	Minimal	
RFC2014014215	CIP-007-3a	R5.1.2	CA		
RFC2014014216	CIP-007-1	R5.2, R5.2.3		Serious	
RFC2014014257	CIP-007-3a	R5.3; R5.3.1, R5.3.2, R5.3.3			
RFC2014014238	CIP-007-3a	R9	CA	Moderate	
RFC2014014239	CIP-008-3	R1.6			
RFC2014014240	CIP-009-3	R1		Serious	
RFC2014014241	CIP-009-3	R2			

NERC Violation ID	Standard	Req	Discovery Method* Date	Risk	Penalty Amount
RFC2015015301	CIP-009-3	R2		Serious	$1,700,000
RFC2014014013	CIP-009-1	R4	SR		
RFC2015015302	CIP-009-3	R4			
RFC2014014242	CIP-009-3	R5	CA		
RFC2015015303	CIP-009-3	R5			

Background

During a Compliance Audit and subsequent enforcement process, ReliabilityFirst determined that URE had serious, systemic security and compliance issues across URE's multiple business units. Additionally, multiple violations were repeats of prior violations. Some of the most significant violations involved patching and physical security. For example, regarding patching under CIP-007-3a R3, URE did not patch its energy management system (EMS) after it completed its mitigation plan for the same violation identified during a previous CIP Compliance Audit. In another example, regarding physical security, URE discovered that three Physical Security Perimeter (PSP) doors to a central control room had been tampered with, presumably by employees, thus preventing the doors from latching securely. URE's most recent issue with securing its PSP occurred when an employee worked eight shifts despite URE revoking the employee's physical access for failure to complete annual requalification training. Of the 36 violations, ReliabilityFirst determined that 21 violations posed a serious and substantial risk to the reliability of the Bulk Power System (BPS), 11 posed a moderate risk to the reliability of the BPS, and the remaining 4 posed a minimal risk to the reliability of the BPS. ReliabilityFirst considered the risk and harm posed by the violations to the reliability of the BPS in the aggregate and determined that these violations collectively posed a serious and substantial risk to the reliability of the BPS.

The root causes of these violations were cultural issues that resulted in URE management's lack of awareness, engagement, and accountability for CIP compliance. Moreover, URE failed to identify its CIP issues, and even after identification, failed to promptly address the CIP issues. URE delayed submitting Mitigation Plans, was late in completing many of its Mitigation Plans, and failed to complete four Mitigation Plans, which resulted in ReliabilityFirst requiring URE to prepare and submit 4 new Mitigation Plans.

ReliabilityFirst notes that URE has recently agreed to work with ReliabilityFirst through at least the second quarter of 2016 to holistically evaluate and work to improve its culture and thus its overall security posture and CIP Compliance Program. URE has committed to ReliabilityFirst that improvements will include increased senior management involvement, reorganization, increased resources, and significant process improvements.

RFC2014014245 CIP-002-3 R3 - OVERVIEW

ReliabilityFirst determined that URE did not provide sufficient evidence of identifying programmable relays as Cyber Assets and URE failed to identify several Critical Assets correctly. First, two switches located at a backup control center were listed by URE as access points, but were actually Critical Cyber Assets (CCAs) and not access points. Second, a server was identified by URE as a CCA, but based on URE's methodology, should have been identified as a non-CCA. Third, a CCA listed on URE's list of CCAs was identified during a site visit of the Compliance Audit, but was not included on URE's pre-audit submission of identified Cyber Assets. In addition, ReliabilityFirst determined that URE did not provide evidence demonstrating an adequate evaluation of programmable relays for CCA identification. This determination was based on a lack of information on URE's pre-audit submissions and subsequent lack of clarity from subject matter expert interviews on the same subject.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Not developing a complete lists of CCAs increased the risk that URE would miss CCAs that were not on the list when implementing the security controls. URE exhibited a lack of processes and procedures to ensure the reliable identification of those devices that are critical. Such process and procedure gaps result in violations that are likely to be repeated. The risk was only partially mitigated because not all of the devices were determined to be CCAs, and were therefore less critical to security.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011422 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise its process for annually reviewing, documenting, and determining whether programmable relays for protective systems are CCAs;
2. update and implement its asset validation process to include validating the classification of each asset on the list of Cyber Assets and to include a review of the entire list of assets to verify each asset has been classified and evaluated correctly; and

3. design an internal pre-specification for completing the Attachment C, which is an input to the pre-audit process for ReliabilityFirst.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014014 CIP-003-1 R6 - OVERVIEW

ReliabilityFirst determined that URE retained an independent vendor to perform a NERC CIP gap analysis, which revealed that URE's process for requesting changes to firewall rules failed to include documentation of changes to firewall rulesets. In addition, during the Compliance Audit, ReliabilityFirst discovered several other instances of failure to establish change control or configuration management. Specifically, URE failed to: a) establish configuration management for its generation business unit; and b) provide evidence of a change control or configuration management program for its information technology services business unit. In both cases, URE stated that it had processes in place, but URE did not provide adequate evidence of processes that would apply to devices randomly selected for the Compliance Audit.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to manage firewalls, a key primary defense for critical systems and operations, increased the risk of malicious activity that could compromise the BPS. In addition, URE's widespread failure to implement change control and configuration management significantly increased the likelihood of failing to restore CCAs in the event of critical failure. Lastly, because the instances of violation were rooted in a lack of configuration management processes, the violations were likely to recur until mitigated.

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.

URE submitted its Mitigation Plan designated RFCMIT011103-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. change its change control and configuration management process to include documentation of firewall rule changes;
2. implement a configuration management system and a configuration management database; and
3. create a process to show the addition of systems within the configuration management database, including initial baselines.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014251 and RFC2014014252 CIP-004-3 R2 and R2.1 - OVERVIEW

RFC2014014251

ReliabilityFirst determined that URE did not review its cyber security training program for two consecutive years. In addition, some training material, specifically a web-based training course, was used for training but was not described in URE's cyber security training program.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk posed by the violation was that URE would inconsistently implement its training program as a result of not reviewing the program and not having all materials used for training actually documented in the training program. A lack of training or inconsistent training was determined to be the root cause of multiple violations resolved through the Settlement Agreement. This risk was only partially mitigated because URE had formal training material and a training program.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE's Mitigation Activities required URE to implement a new cyber security training program.

ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014252

ReliabilityFirst determined that URE did not provide evidence that contractors and service vendors were trained prior to being granted access to CCAs. In addition, URE failed to provide evidence that training was conducted at least annually. URE provided evidence forms that did not include training dates and evidence indicating that some personnel were granted access to CCAs prior to receiving training.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. During the Compliance Audit, URE had difficulty producing training data, indicating that this issue has a high likelihood of recurrence. In addition, there were multiple variations of issues with incomplete training documentation and failure to train during the required timeframes, indicating that URE had multiple process weaknesses in managing cyber security training records. These process

weaknesses could lead to a general lack of awareness of cyber security issues across the organization and its contracted staff. Additionally, insufficient training may degrade URE's ability to prevent and respond to cyber security incidents.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011538 to address the referenced violations. URE's Mitigation Plan required URE to address the root cause of the violation by identifying a single internal organization, the NERC Training Organization, to be responsible for all URE cyber security training and implementing a technology solution to enable non-badged vendors and contractors who previously fell into process gaps to complete cyber security training through a web-based delivery system.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014253 CIP-004-3 R3.3 - OVERVIEW

ReliabilityFirst determined that URE did not ensure that each Personnel Risk Assessment (PRA) included the date that the assessment was conducted, or that the PRA included a seven-year criminal check. This was consistent with all contractors and vendors ReliabilityFirst sampled during the Compliance Audit. URE obtained PRA data through a self-designed form provided to its vendors, but URE failed to collect sufficient information through its process to demonstrate compliance with CIP-004-3 R3.3. Additionally, ReliabilityFirst noted that the evidence provided was inconsistent and incomplete as a result of the siloed nature of the business units preparing the data and a lack of final review before submitting the evidence.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Not ensuring that all contractors and vendors have PRAs potentially made URE susceptible to malicious acts by insiders, and the long duration of the violation increased this risk of harm. In addition, the root cause of the violation involved an ineffective process, which can lead to multiple instances of noncompliance. The risk was only partially mitigated because URE did have a process in place, although it was inadequate, and did require some evidence of background checks, although the evidence was insufficient.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011548 to address the referenced violations. URE's Mitigation Plan required URE to:

1. perform an internal audit to ensure its contractors and vendors had completed PRAs; and
2. update its process to ensure that, going forward, PRAs are completed consistently with NERC Standards, including an effort to ensure that attestations from contractors and vendors are accurate and to identify more effective methods of collecting PRA information from third parties.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2013013197, RFC2014013447, and RFC2014013997 CIP-004-3a R4.2 - OVERVIEW

RFC2013013197

ReliabilityFirst determined that URE did not maintain its list of personnel with authorized cyber or authorized unescorted physical access to CCAs when it failed to revoke access to CCAs for two individuals within seven calendar days of those individuals no longer requiring access to CCAs. In the first instance, URE did not revoke an employee's physical access to CCAs when the employee changed positions within URE and therefore no longer required access to CCAs. In the second instance, URE did not revoke an employee's physical access to CCAs when the employee's training qualifications lapsed, which URE identified as an instance of an employee no longer requiring access.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Not revoking access when it is no longer needed leads to increased risk of unwarranted access to those CCAs, and this type of violation was likely to recur as the root cause related to an effective process. The risk was partially mitigated because, in both instances, URE had conducted PRAs on the employees and both PRAs were current and up-to-date. Additionally, both employees received proper training prior to being granted access to CCAs.

ReliabilityFirst determined the duration of the first instance to be from the date the first employee no longer required access to CCAs, through when URE revoked the employee's access. ReliabilityFirst determined the duration of the second instance to be from the date the second employee no longer required access to CCAs, through when URE revoked the employee's access.

URE submitted its Mitigation Activities within its Self-Reports. At the time of the violation, ReliabilityFirst believed this mitigation was sufficient because the root cause initially appeared to be an

isolated human error issue. However, URE later determined that the root cause was broader and related to ineffective processes, and thus URE later corrected this root cause through its subsequent Mitigation Plans under RFC2014013447 and RFC2014013997.

URE certified that it had completed its Mitigation Activities, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014013447

ReliabilityFirst determined that during user access review, physical access for one retired employee had not been revoked within seven calendar days of the employee no longer requiring access to a CCA. URE revoked physical access for this retired employee upon discovery and verified that the retired employee did not have cyber access.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's not revoking access when it is no longer needed leads to increased risk of unwarranted access to those CCAs, and this type of violation was likely to recur as the root cause related to an ineffective process. The risk was partially mitigated because the employee was properly trained prior to gaining access, had a current PRA, and did not have any cyber access to any CCAs.

ReliabilityFirst determined the duration of the violation to be from the date URE should have revoked access to the CCA, through when URE revoked the access.

URE submitted its Mitigation Plan designated RFCMIT010551 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revoke physical access;
2. coach employees on proper revocation procedures;
3. review the efficacy of the revocation process; and
4. implement improvements identified from the process review, including implementation of a new tool to assist with revocation.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014013997

ReliabilityFirst determined that in preparation for the Compliance Audit, URE completed a review of access records and discovered two instances in which physical access was not revoked within seven

calendar days. In one instance, URE was four days late in revoking access, and in the second instance, URE was 46 days late.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE failed to identify the violation outside the scope of an upcoming Audit, and URE demonstrated a lack of internal controls to quickly identify procedural failures. In addition, although the subjects of the Self-Report had only physical access to CCAs, not revoking access when it is no longer needed leads to increased risk of unwarranted access to those CCAs, and this type of violation was likely to recur as the root cause related to an ineffective process. The risk was partially mitigated because the individuals whose access had not been revoked had updated training and PRAs.

ReliabilityFirst determined the duration of the violation to be from the date URE was required to revoke access, through when URE revoked the access.

URE submitted its Mitigation Plan designated RFCMIT011102-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. complete a root cause analysis and document the process for provisioning and revoking access; and
2. create a process flow diagram, identify correct roles and responsibilities, and implement the process.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014013623, RFC2014014015, RFC2014014207, and RFC2015015300 CIP-005-3a R1.5 and R1.6 - OVERVIEW

RFC2014013623

ReliabilityFirst determined that URE did not identify a certain class of routers and switches (Lightweight Directory Access Protocol, or LDAP) as being used in the access control and/or monitoring of the Electronic Security Perimeter (ESP) and therefore failed to afford the protective measures specified in CIP-005-3a R1.5.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. By not protecting the devices used for access control into the ESP, the ESP could be

compromised. Additionally, the violation occurred due to URE's misunderstanding of the applicability of the Standards and the duration was long before URE realized the error.

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.

URE submitted its Mitigation Plan designated RFCMIT010669 to address the referenced violations. URE's Mitigation Plan required URE to:

1. eliminate the LDAP system as the sole authentication system to gain access to routers and switches within the ESP; and
2. implement a new scheme that uses two-factor authentication to access a jump box, which serves as the sole access point into the ESP.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014015

ReliabilityFirst determined that URE identified its Security Information and Event Management (SIEM) system, which is located in its Corporate Data Center, as a Cyber Asset used in the access control and/or monitoring of an ESP, but failed to maintain a PSP around the Corporate Data Center.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to properly identify all protections necessary for a new Cyber Asset, the room that contained the SIEM system did have physical access protections such as continuous access control and monitoring through the use of card readers and security staffing. As a result, the Corporate Data Center had the same protective measures required by CIP-006-3c R3 despite the lack of a PSP designation.

ReliabilityFirst determined the duration of the violation to be from the date the URE installed the SIEM system that gave rise to the requirement to identify the Corporate Data Center as a PSP, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011099 to address the referenced violations. URE's Mitigation Plan required URE to create a PSP around the Corporate Data Center, and the SIEM system and other newer Cyber Assets were validated as being within the boundaries of a PSP.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014207 and RFC2015015300

ReliabilityFirst determined that URE did not properly maintain documentation of CCAs and non-CCAs within ESPs. Specifically, ReliabilityFirst discovered two problems with drawings submitted by URE for the Compliance Audit. First, a CCA on the list of NERC CIP Cyber Assets was not found on the corresponding drawings. Second, two other CCAs on the NERC CIP Cyber Assets list did not appear on the drawings, but were found to have changed names. URE submitted to ReliabilityFirst a Mitigation Plan to address the Alleged Violation of CIP-005-3 R1.6 (RFC2014014207) and committed to complete the Mitigation Plan. However, despite ReliabilityFirst's onsite and offsite verification efforts, ReliabilityFirst could not reasonably verify that URE completed its Mitigation Plan. Thus, ReliabilityFirst determined that the underlying violation was not sufficiently addressed and was ongoing. As a result, ReliabilityFirst found a new violation for failure to mitigate (RFC2015015300) and required URE to submit a new Mitigation Plan to address the underlying violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Although the violation was only a documentation issue, it was indicative of a larger procedural issue with a long duration and thus was likely to recur. Also, through ReliabilityFirst's Mitigation Plan verification efforts, ReliabilityFirst determined that URE inaccurately identified devices in its ESP and PSP drawings and therefore lacked a basic understanding of its ESPs, thus increasing the risk that URE's ESPs would not be effective and would allow for potential compromise of its CCAs.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its subsequent Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011828 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise its existing list of CCAs to include related ESP and PSP designations; and
2. develop documents and implement a process to ensure that ESP, PSP, and asset type information is regularly validated and associated lists are updated to reflect the production environment.

RFC2014014410, RFC2015015143, RFC2014014011, and RFC2014014208 CIP-006-3c R1, R1.1 and R1.8 - OVERVIEW

RFC2014014410

ReliabilityFirst determined that an employee escorting a vendor into URE's System Operations Center left the vendor unescorted for a short period of time in order to place a phone call. The vendor was discovered by URE security and escorted by security for the remainder of his time onsite to complete maintenance work for which he was contracted.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had a visitor escort policy in place, and the violation appears to be an isolated human performance issue that was quickly identified and corrected by URE security.

ReliabilityFirst determined the duration of the violation to be the one day when URE failed to follow proper internal procedures while escorting a vendor.

URE submitted its Mitigation Plan designated RFCMIT011776-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. discipline the employee through the corporate positive discipline process; and
2. enhance its training program to include example violations relating to visitor escort procedures.

RFC2015015143

ReliabilityFirst determined that URE terminated an employee's physical access for failure to complete annual requalification training. However, the employee continued to work eight shifts in a power plant control room in a PSP despite not having physical access because other employees permitted him access. Later, the employee made multiple attempts to access the PSP by swiping his access card, which triggered an alarm in the plant security office. This alarm was the result of a newly developed control to alert security in case of three failed access attempts by the same person within an hour. A security officer investigated the alarm and found the employee in the control room. URE later learned that the employee's annual requalification training was almost past due and the access provisioner prematurely revoked access as a result of an error in the notification report identifying employees whose training was set to expire.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk that this specific employee would put the BPS at risk is low because the employee had a current PRA and no cyber access. Moreover, the employee's access to the PSP

was removed only as a result of failure to timely complete annual requalification training as opposed to a termination, which may increase the risk that the employee would use the access in such a way as to put the BPS at risk. However, the violation is indicative of a poor compliance culture as the employee continued to work eight shifts even though his access was removed and other employees allowed him access even though his access was removed. The cultural issue, if not fixed, could lead to other violations in the future.

ReliabilityFirst determined the duration of the violation to be from the first day the employee was permitted in the PSP despite having his access revoked, through the day the employee's access was reinstated as a result of completing his training.

URE submitted its Mitigation Plan designated RFCMIT011743-3 to address the referenced violations. URE's Mitigation Plan required URE to:

1. provide the employee with training and URE reinstated the employee's access;
2. place a visual indicator inside all control rooms near the inside exit buttons to remind personnel opening the door to log and escort visitors;
3. conducted training for all CIP plant employees with respect to procedures for visitors;
4. modify the early notification report to the access provisioner to clearly distinguish between expired training and training that will expire; and
5. develop a process to proactively reassign work for individuals whose access will be revoked so that the individuals can work outside of the PSPs.

RFC2014014011

ReliabilityFirst determined that 13 separate openings in a six-wall border exceeded 96 square inches. Two openings of approximately 1,440 square inches each were discovered at one generating facility, a third opening of approximately 240 square inches was discovered at another generating facility, and the remaining ten openings of approximately 130 square inches were discovered at URE's a separate operations center. URE determined that the openings were a result of original construction conditions, with the exception of the 240 square inch opening, which was created during a repair of a water leak within the PSP at the facility.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Most of the 13 openings were sufficiently small and hidden so as to render penetration of the PSP unlikely. However, two of the openings were larger and allowed sufficient

space for penetration of the PSP. Additionally, the four-year duration of the violation indicates a general lack of rigor in URE's Compliance Program.

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.

URE submitted its Mitigation Plan designated RFCMIT011101-1 to address the referenced violations. URE's Mitigation Plan required URE to remediate each of the openings, document a new process for performing work on PSPs to include contacting security to ensure compliance, and update the work management checklist used when work is completed on PSPs.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014208

ReliabilityFirst determined that URE did not annually review certain documents used to support URE's physical security plan. Specifically, URE did not review 13 "as-built drawings," which URE identified as documents that detail the specifications of each PSP. During the audit, URE stated that the drawings are reviewed on an ad-hoc basis rather than annually.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Despite having a process in place that required review of the drawings, URE personnel failed to follow the policy, indicating a lack of focus on physical security, or compliance generally. Although the drawings were not reviewed annually as required by CIP-006 R1.8, URE attests that the drawings were reviewed during the duration of the violation.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011545 to address the referenced violations. URE's Mitigation Plan required URE to clarify the scope of the annual review of the physical security plan in its process documents and create a related review checklist for the annual review.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014209 and RFC2013013198 CIP-006-3a R5 and CIP-006-3c R5 - OVERVIEW

RFC2014014209

ReliabilityFirst determined that URE's physical security plan uses too narrow a definition of the term "unauthorized access attempts." During the Compliance Audit, URE subject matter experts explained that URE's determination that no unauthorized access attempts took place relied on URE's definition of an "unauthorized access attempt" as not including invalid attempts. URE defines "unauthorized access attempts" as either tailgating, access gained without authorization, or a visitor separated from an escort. These thresholds would not include failed attempts to access a secure area and therefore only would identify successful attempts at unauthorized entry, falling short of the requirement to monitor physical access to PSPs.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's definition of unauthorized access attempts include only successful security breaches and not attempts to access the PSP. Thus, URE's practice of relying on successful unauthorized access can lead to delayed detection and response to malicious activity.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011544 to address the referenced violations. URE's Mitigation Plan required URE to modify its relevant security procedure to instruct security officers to investigate cases of multiple failed access card-key reads at PSPs, in addition to the requirement of investigating cases of tampering and piggybacking.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2013013198

ReliabilityFirst determined that while performing a monthly physical barrier inspection of a PSP at a power plant, a security officer discovered that three PSP doors to a central control room had been tampered with, thus preventing the doors from latching securely. As a result, the security officer was able to open the doors without swiping an authorized access card-key. The security officer also determined that although a door-forced alarm should have sounded, it in fact did not operate. URE performed a root cause analysis and traced the cause of the alarm failure to a firmware upgrade. Although URE followed the established procedure for the upgrade, the vendor determined through this root cause analysis that an additional step was needed to clear device memory before conducting

the upgrade. URE also conducted an investigation with respect to the door tampering, but the investigation was inconclusive with respect to the reason for the tampering. As a result of this incident at the power plant, URE subsequently tested the alarm functionality of all PSP access points and discovered issues with two additional PSP access points at its System Operations Center, where the alarming system failed due to faulty wiring and hardware. URE also discovered issues with seven PSP access points at its Alternate System Operations Center and one access point at another power plant.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The initiating action in this violation, an ongoing physical tampering of security systems, is a significant culture of compliance breakdown. In addition, although URE did eventually discover the issue through the implementation of internal detective controls, the condition was not discovered timely. Thus, the violation potentially put the BPS at serious risk for a long duration.

ReliabilityFirst determined the duration of the violation to be from the date the URE's firmware upgrade first affected its alarming capability, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT010465 to address the referenced violations. URE's Mitigation Plan required URE to:

1. initiate its alternate security measures, which include dispatching a security officer to perform a roaming security patrols around the PSP;
2. perform a root cause analysis, restore alarm functionality to the doors at the generation plant Control Room, replace the portion of hardware that malfunctioned, and redistribute the configuration data for the access points;
3. test the alarm functionality of these access points on a weekly basis for several months to ensure the alarms continued functioning properly;
4. test the alarm functionality of all 105 URE PSP access points and perform a network walk down which consisted of a visual inspection of all computer equipment in the relevant control room, validation of known computer equipment, and a search for any anomalies; and
5. provide refresher access training presentations to personnel at the power plant in question.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014211 CIP-007-3a R1.3 - OVERVIEW

ReliabilityFirst determined that URE did not provide evidence of testing for cyber security controls for one Cyber Asset. The device not tested was a virtual server located at a power plant. URE indicated that its vendor tests the device, but URE did not provide ReliabilityFirst with evidence of such a test.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. A failure to test security controls on new Cyber Assets and those with significant changes can result in the affected Cyber Assets failing to perform as expected. URE failed to detect a lack of security controls testing by its vendor, at least in part because URE failed to maintain policies or procedures that govern vendor testing. This lack of oversight led to a long running violation that is likely to recur in multiple ways due to a lack of process and procedure.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011541 to address the referenced violations. URE's Mitigation Plan required URE to assign an individual as a subject matter expert role for the group responsible for testing the Cyber Asset at issue, build an in-house test system, and update related documentation.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014013998 CIP-007-1 R2 - OVERVIEW

ReliabilityFirst determined that URE did not ensure that only those ports and services required for normal and emergency operations were enabled. Specifically, URE lacked documentation identifying the ports and services required for normal and emergency operations for three Net Controllers managed by URE's information technology services organization (ITS), two operator interface server systems managed by URE's generation unit, and 18 paperless chart recorders within the generation unit.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Without proper documentation on ports and services, URE could not confirm whether it enabled only ports and services required for normal and emergency operations. Thus, URE could have had ports and services enabled that were not required for normal or emergency operation, which would have created vulnerabilities that expose the systems to a higher risk of compromise by potentially allowing more channels for undetected access into URE's critical systems. Given this risk, and the fact

that the violation would have continued except for preparation of evidence for the Compliance Audit, the risk to the BPS was serious and substantial.

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.

URE submitted its Mitigation Plan designated RFCMIT011100-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. complete a baseline of ports and services for the operator interface server assets and Net Controllers and remove the paperless chart recorders from the ESP; and
2. revise the Technical Feasiblibility Exception (TFE) process to clarify expectations and allow subject matter experts to access existing TFEs.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014013626, RFC2014014262 and RFC20141014114 CIP-007 R3, R3.1, R3.2 - OVERVIEW

RFC2014013626

ReliabilityFirst determined that URE did not assess patches for its routers and switches, of which there are approximately 50, within its ESP because URE did not interpret CIP-007-1 R3 to require assessments of firmware upgrades, which require the entire upgrade of the operating environment rather than the application of a single software patch targeted to solve a vulnerability. URE indicated that it conducted periodic, undocumented reviews of firmware releases.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS.

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.

URE submitted its Mitigation Plan designated RFCMIT011578-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. assess all networking devices for patch applicability;
2. perform industry survey to understand how other utilities manage security patching for these devices;

3. establish a process for assessing the firmware;
4. replace hardware and upgrade other devices where necessary; and
5. run monthly reports on network firmware that check for the current version of network firmware.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014114 and RFC2014014262

Regarding CIP-007-3a R3.2, URE did not document the implementation of applicable security patches for its server devices (which host URE's EMS applications), the date it last patched those devices as part of its mitigation for the same violation identified during its CIP Compliance Audit. In total, there were 75 security patches released for URE's EMS. URE indicated that a contributing cause for this violation was that it did not have a process map that clearly indicates the process for patch management.

Regarding CIP-007-3a R3.1, URE did not assess patches or security upgrades for its firewalls. In addition, when security patches were not applied, URE did not document compensating or mitigating measures. URE had interpreted that firewalls were not Electronic Access Control or Monitoring Systems (EACMS). Based upon this interpretation, URE protected these devices based on CIP-005 Requirements but did not follow the CIP-007 Requirements applicable to EACMS.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's EMS has a direct impact on the reliability of the BPS, and not patching it since its mitigation for its previous CIP audit (during which time 75 patches were released) left the system vulnerable and put the BPS at serious risk of exploitation. Additionally, firewalls are one of the primary security controls against realization of potential threats and compromise, and not patching them left the system vulnerable and put the BPS at serious risk of exploitation.

ReliabilityFirst determined the duration of the violation to be from the date URE last patched its EMS, through when URE completed its Mitigation Plan.

For RFC2014014114

URE submitted its Mitigation Plan designated RFCMIT011526 to address the referenced violation. URE's Mitigation Plan required URE to:

1. assess and install applicable patches and apply for TFEs where applicable and implement compensating measures;
2. increase staff assigned to patching processes and develop a process to ensure ongoing knowledge and staff availability for implementing patches; and
3. develop a comprehensive TFE process and improve its patch management process to clarify deadlines and actions required.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

For RFC2014014262

URE submitted its Mitigation Plan designated RFCMIT011537 to address the referenced violation. URE's Mitigation Plan required URE to:

1. assess all security updates for firewalls identified as cyber assets, and institute a process for periodic assessment updates and evidence submissions;
2. define a standard for EACMS that includes the firewalls at issue; and
3. update its work documents to provide common work instructions for managing patch management activities for firewalls.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014012 CIP-007-3a R4 - OVERVIEW

ReliabilityFirst determined that two SIEM devices, which are Cyber Assets used in the access control and/or monitoring of the ESP, are not technically capable of complying with CIP-007-3a R4 as they cannot implement antivirus software or other malicious software prevention tools. However, URE did not file a Technical Feasibility Exception (TFE) with ReliabilityFirst. URE has documentation from the vendor documenting the compensating measures applied to the SIEM devices to mitigate risk exposure.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This violation was a documentation issue as the SIEM device could not support antivirus or other malicious software prevention tools and the vendor has documented compensating

measures applied to the SIEM devices to mitigate risk exposure. Thus, there was no increased risk of harm to the BPS as a result of URE not applying for a TFE with ReliabilityFirst.

ReliabilityFirst determined the duration of the violation to be from the date URE deployed its SIEM system, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011105 to address the referenced violations. URE's Mitigation Plan required URE to amend an already approved TFE with ReliabilityFirst to include the documented compensating measures applied to mitigate risk exposure from the inception of the SIEM devices.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014215, RFC2014014216, and RFC2014014257 CIP-007-3a R5.1.2, R5.2, R5.2.3, R5.3, R5.3.1, R5.3.2, R5.3.3 - OVERVIEW

RFC2014014215

ReliabilityFirst determined that URE did not provide logs of user account activity for a minimum of 90 days. URE did not have logs for a certain device sampled by ReliabilityFirst during the Compliance Audit. The device stopped communicating with the SIEM system for 15 days. URE asserted that although the device was not communicating with the SIEM system, local logs could be provided from the device. However, ReliabilityFirst determined that the application logs did not provide sufficient evidence that logs of sufficient audit trails were created.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Inadequate audit trails of user actions on CCAs can lead to missing cyber security events. However, the violation applied to only one device, and URE had logs, although the logs did not have sufficient detail.

ReliabilityFirst determined the duration of the violation to be the time during which URE could not provide logs of user account activity.

URE submitted its Mitigation Plan designated RFCMIT011534-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. update the job aid to clearly define steps that should be taken in the event of a logging failure detection;

2. change the process so that the alert goes directly to security, then to the specific business unit at issue; and
3. improve the agent-based logging failure detection trigger criteria to 24 hours.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014216

ReliabilityFirst determined that URE did not properly manage the scope and acceptable use of administrator, shared, and other generic account privileges, including factory default accounts. In addition, URE did not maintain an audit trail of the account use of administrator, shared, and other generic account privileges, including factory default accounts. More specifically, regarding CIP-007-3a R5.2, at one of URE's power stations, during the Compliance Audit, ReliabilityFirst found labels attached to a device monitor in the central control room that provided the shared account Username and Password required to gain initial access to the device after startup. URE conducted a thorough root cause analysis.

First, URE determined that a shared account was used when initiating the Remote Desktop Protocol sessions before the generation software was initiated because if individual accounts were used, it would require the operator to log out of the operating system session when control of the unit was to exchange hands, which in turn would terminate the generation application and create potential risk to the Critical Asset by terminating the operator's ability to maintain control of the Critical Asset. URE determined that the shared operating system account had limited privileges and the application deemed to be of highest risk in use under that shared operating system account had application level authentication implemented and authentication logged. Thus, URE believed that it could meet the requirement of tracking who had access to this shared account by using the generation application's user authentication logs.

Regarding CIP-007-3a R5.2.3, URE had a policy that requires an audit trail of accounts use. However, URE could not provide ReliabilityFirst with evidence of an audit trail for shared accounts. URE asserted that it did not interpret the requirement correctly and could not provide an audit trail of individual access to shared accounts. URE's interpretation was that it was required to log the "identity of which users can use the shared accounts," rather than to "identify users who did use the shared account" each time a shared account is used.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Regarding the shared username and password, inadequate shared account management can lead to inadvertent use of CCAs, which can result in compromise of CCAs. The risk posed by the discrete violation may have been partially reduced because of the limited privileges in the shared account and additional authentication required to access the critical software on the device. However, the overall risk posed by the violation is serious and substantial, because the contributing factors to the violation, the process gaps and lack of awareness as to CIP requirements by the individuals implementing the CIP Compliance Program, could have led to other violations. Regarding the individual audit trails, inadequate audit trails can lead to missing cyber security events, and URE did not track individual use at all.

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.

URE submitted its Mitigation Plan designated RFCMIT011467-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. schedule quarterly clean desk walk downs at each plant to ensure no passwords or user identifications are posted;
2. validate the need for all current shared accounts;
3. implement a process for logging and review of logs for individual use of shared accounts and training on the process; and
4. install individual accounts and remove shared operator accounts for devices at issue.

RFC2014014257

ReliabilityFirst determined that URE did not meet the password requirements on all Cyber Assets and did not file a TFE where applicable. More specifically, first, for routers and switches, URE uses a jump box to reach the devices. Authentication occurs at the jump box, which uses corporate active directory. There is a built-in user identification that is used when the jump box is not available and the password parameters for this account are not set as per R5.3.1, R5.3.2, and R5.3.3. Second, for servers in URE's System Operations Center, those servers have shared accounts for which passwords were not changed in two consecutive years. Third, for Net Controllers used by the Physical Access Control Systems (PACS), it is not technically feasible to set password parameters on these devices. While URE has a TFE for password complexity, it did not submit a TFE for minimum characters of a password (R5.3.1) or annual password changes (R5.3.3).

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Use of built-in accounts along with weak passwords, and not timely changing passwords, increases the risk that malicious actors will discover passwords and compromise CCA information as it makes passwords easier to decipher and allows malicious actors more time to decipher passwords. Additionally, the root causes of the violations were systemic issues with processes surrounding passwords management and the TFE process and thus could result in additional violations.

ReliabilityFirst determined the duration of the violation to be from the last day of the previous Compliance Audit of URE for the CIP Reliability Standards, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011543 to address the referenced violations. URE's Mitigation Plan required URE to:

1. reset all server shared accounts;
2. compile a list of filed TFEs;
3. develop a process for creation, maintenance, and reference of TFEs;
4. establish an annual, manual password change process for shared accounts; and
5. develop a centralized account management process which includes comprehensive password management.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014238 CIP-007-3a R9 - OVERVIEW

ReliabilityFirst determined that URE did not review and update documentation specified in CIP-007-3a at least annually for seven of the sixteen documents sampled during the Compliance Audit. Specifically, URE did not conduct: 1) an annual review of information technology services organization NERC-CIP testing procedure; 2) a review of Preferred Provider Organizations (PPO) 291 testing procedures for CCAs; 3) an annual review of ITS-SCADA patch management susceptibility weight imaging (SWI); 4) an annual review of the NERC CIP requesting access to a critical and/or non-CCAs within the ESP document ; 5) an annual review of the PPO 289 managing and controlling CIP secured access document; 6) an annual review of the NERC-CIP shared access SWI document; and 7) an annual review of the NERC-CIP account password requirements SWI document.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The root cause related to process gaps, indicating that the issues would have continued and additional reviews would have been missed. Not conducting annual reviews posed a risk that the procedures would not be updated as required, thus potentially leading to other violations.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011535 to address the referenced violations. URE's Mitigation Plan required URE to:

1. identify a complete inventory of CIP-007 related documents and begin tracking all relevant documents in a compliance tracking tool that sends automatic notifications to document owners relating to reviews; and
2. develop a process to review and update documentation at least annually for the required documents.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014239 CIP-008-3 R1.6 - OVERVIEW

As evidence that URE tested its ITS Incident Response Plan, URE submitted documents relating to a paper drill exercise. However, ReliabilityFirst determined that URE was unable to establish how this exercise demonstrated testing of the ITS incident response plan. URE noted that there was not a one-to-one mapping of the exercise to the ITS incident response plan, but rather the subject matter experts were expected to know the plan and follow it during the exercise. Though the evidence reflected a paper drill exercise, it did not demonstrate sufficient and appropriate evidence for testing the ITS incident response plan. URE's ITS business unit did not have a standard that specified how the annual ITS incident response plan test shall be executed to ensure the exercise is compliant with the CIP-008 standard.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE needs to completely test, and adjust as necessary, the ITS incident response plan to ensure the plan will be effective in an actual security incident. However, this risk was partially mitigated by the fact that URE's ITS incident response plan otherwise met the CIP-008-3 Requirements and URE attempted to perform an annual test of the incident response plan, thus reducing the risk that the plan would be ineffective in case of an actual security incident.

ReliabilityFirst determined the duration of the violation to be from the date by which URE was required to test its ITS incident response plan through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011519-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop a pre-specification defining the required level of evidence to comply with CIP-008;
2. develop the standard for proper execution of the incident response plan exercise;
3. update the incident response plan to remove inaccurate language indicating that certain actions were voluntary;
4. execute the updated required annual exercise; and
5. define an effective evidence test procedure to ensure the evidence collected during the annual exercise meeting the pre-specification.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014240 CIP-009-3 R1 - OVERVIEW

ReliabilityFirst determined that URE did not include all CCAs, such as storage area network (SAN) switches, within its ITS recovery plan. The switches were overlooked because the ITS recovery plan concentrated on only the application layer of the CCAs, and URE did not have a sufficient process for validating that the ITS recovery plan included all CCAs. Also, URE did not demonstrate evidence of an annual review of the ITS recovery plan.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Not having sufficient information on CCAs in its ITS recovery plan could have prevented URE from restoring CCAs' functionality. Additionally, the lack of an annual review increased the risk that the ITS recovery plan would continue to be insufficient because URE would not have the opportunity to identify the deficiencies in order to correct them. SAN switches are critical pieces of equipment that are necessary to provide connectivity to SAN storage, which is used by the EMS. Lack of an adequate recovery plan or information related to these CCAs could cause significant delays in recovery of essential assets supporting the BPS.

ReliabilityFirst determined the duration of the violation to be from the date by which URE was required to conduct an annual review of the ITS recovery plan, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011542 to address the referenced violations. URE's Mitigation Plan required URE to update the ITS recovery plan to ensure it covers all CCAs and revise its asset validation process to reconcile and review the ITS recovery plan to ensure it covered all CCAs.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014241 and RFC2015015301 CIP-009-3 R2 - OVERVIEW

ReliabilityFirst determined that URE did not provide sufficient evidence that it annually tested its recovery plans for its generation and ITS business units or its EMS. While URE submitted some evidence of URE's testing of the recovery plans, the evidence was insufficient. URE submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-009-3 R2 and committed to complete the Mitigation Plan by a certain date. However, despite ReliabilityFirst's onsite and offsite verification efforts, ReliabilityFirst could not reasonably verify that URE completed its Mitigation Plan on the assigned date. Thus, ReliabilityFirst determined that the underlying violation was not sufficiently addressed and was ongoing. As a result, ReliabilityFirst found a new violation (RFC2015015301) for failure to mitigate and required URE to submit a new Mitigation Plan to address the underlying violation.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. URE demonstrated a lack of understanding of what is required to exercise its recovery plans such that they could be relied on during an actual recovery situation. Thus, this, along with not having adequate documentation to cover all CCAs within the recovery plans, presented the risk that there could have been gaps in recovery capability, or delayed recovery during an actual event, which could have caused serious harm to the reliability of the BPS.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period through when URE completed its subsequent Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011829 to address the referenced violations. URE's Mitigation Plan required URE to:

1. create one corporate-level recovery plan for BPS cyber systems and subsequent standardized recovery "sub-plans" for each Cyber Asset type;
2. have a defined standardized process for testing each of the recovery sub-plans;

3. include the process for testing a representative sample of information used to recover BPS cyber system functionality and the timeframe in which the test must occur; and
4. conduct recovery exercises for each of the recovery sub-plans.

RFC2014014013 and RFC2015015302 CIP-009-1 R4 and CIP-009-3 R4 - OVERVIEW

ReliabilityFirst determined that URE's ITS business units did not store on backup media information essential to successfully restore CCAs, including the EMS. URE's generation business unit did not store on backup media information essential to successfully restore CCAs, including eight operator control clients and four operator interface server assets. URE's EMS application continuity plan stated that the "active/active" site configuration and site switchover constitutes its ability to backup and restore. This configuration is commonly referred to as "N-1" (redundancy) and is not considered sufficient for back-up and restoration of CCAs.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. In order to accomplish the restoration of functionality of a CCA, URE needed to obtain the essential information to recover the asset and re-establish the functionality previously served by the failed asset. If URE would have lost a CCA, the information to recover the asset would not have been identified and available, hindering timely recovery of that CCA. The CCAs for which URE did not perform backup were essential to the reliable operation of the BPS and thus could have caused serious harm if not timely restored.

ReliabilityFirst determined the duration of the violation to be from the date by which URE committed to complete its initial Mitigation Plan, through when URE completed its subsequent Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011830 to address the referenced violations. URE's Mitigation Plan required URE to:

1. create one corporate level Recovery Plan for BPS cyber systems and subsequent standardized recovery "sub-plans" for each Cyber Asset type;
2. define standardized processes for testing each of the recovery sub-plans;
3. develop a specific recovery sub-plan that addresses specific recovery procedures and media testing procedures for new Version 5 generation systems and associated PACS and EACMS; and
4. conduct recovery exercises for the Recovery Sub-Plans.

RFC2014014242 and RFC2015015303 CIP-009-3 R5 - OVERVIEW

ReliabilityFirst determined that URE did not store on backup media information essential to successfully restore CCAs under CIP-009-1 R4; thus, it could not perform annual testing of that back-up media. URE submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-009-3 R5 and committed to complete the Mitigation Plan by a certain date. However, despite ReliabilityFirst's onsite and offsite verification efforts, ReliabilityFirst could not reasonably verify that URE completed its Mitigation Plan on the determined date. Thus, ReliabilityFirst determined that the underlying violation was not sufficiently addressed and was ongoing. As a result, ReliabilityFirst found a new violation (RFC2015015303) for failure to mitigate and required URE to submit a new Mitigation Plan to address the underlying violation.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. In order to accomplish the restoration of functionality of a CCA, URE needed to obtain the essential information to recover the asset and re-establish the functionality previously served by the failed asset. If URE would have lost a CCA, the information to recover the asset would not have been identified and available as a result of no testing to ensure the backup media would be usable, hindering timely recovery of that CCA. The CCAs for which URE did not perform backup were essential to the reliable operation of the BPS and thus could have caused serious harm if not timely restored.

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

URE submitted its Mitigation Plan designated RFCMIT011827-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. create one corporate-level recovery plan for BPS cyber systems and subsequent standardized recovery "sub-plans" for each Cyber Asset type;
2. define standardized process for testing each of the recovery sub-plans;
3. develop a specific recovery sub-plan that addresses specific recovery procedures and media testing procedures for EMS and associated PACS and EACMS;
4. conduct recovery exercises for at least one asset;
5. type within each recovery sub-plans; and
6. exercise a media test procedure for at least one asset for each recovery sub-plan medium type.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of one million seven hundred thousand dollars ($1,700,000) for the referenced violations. Additionally, ReliabilityFirst will perform a Spot Check of URE in 2016 to review URE's current state of compliance for a targeted sample of CIP Reliability Standard Requirements relating to some of the violations resolved in the Settlement Agreement that posed a serious and substantial risk to the reliability of the BPS.

In reaching this determination, ReliabilityFirst considered the following factors:

1. ReliabilityFirst considered 21 of the instant violations as repeat noncompliance with the subject NERC Reliability Standards for CIP-002 R3, CIP-004 R2, CIP-004 R3, CIP-004 R4, CIP-005 R1, CIP-006 R1, CIP-007 R1, CIP-007 R2, CIP-007 R3, CIP-007 R4, CIP-007 R5, and CIP-009 R1;
2. URE did not have a properly structured internal compliance program at the time of the violations, and ReliabilityFirst did not award any mitigating or above and beyond credit for improvements for the current commitments to improve its culture given the nature of the violations, the long duration of the violations, and URE's slow response to the violations;
3. ReliabilityFirst awarded mitigating credit for URE's implementation of an application to automate some steps for access revocation and provisioning;[2]
4. URE self-reported 17 violations (RFC2014014014, RFC2013013197, RFC2014013447, RFC2014013997, RFC2014013623, RFC2014014015, RFC2014014410, RFC2014014011, RFC2015015143, RFC2013013198, RFC2014013998, RFC2014013626, RFC2014014262, RFC2014014114, RFC2014014012, RFC2014014013, and RFC2015015302), although most of those Self-Reports were submitted to ReliabilityFirst leading up to and following the Compliance Audit. 19 violations were found during a Compliance Audit (RFC2014014245, RFC2014014251, RFC2014014252, RFC2014014253, RFC2014014207, RFC2015015300, RFC2014014208, RFC2014014209, RFC2014014211, RFC2014014215, RFC2014014216, RFC2014014257, RFC2014014238, RFC2014014239, RFC2014014240, RFC2014014241, RFC2015015301, RFC2014014242, and RFC2015015303);

[2] The application includes alerts and controls to help maintain compliance with respect to such things as provisioning the correct level of access, requiring training prior to provisioning access, and timely revoking access where required. Additionally, URE is in the process of implementing a tool to automate and track requests for password changes, logs access, and the usage of privileged accounts. These tools enhance security and reliability beyond that which is required by the CIP Reliability Standards.

5. URE received some mitigating credit for URE's submission of some Self-Reports that were submitted well in advance of the Compliance Audit;
6. URE was not cooperative throughout the compliance enforcement process, and ReliabilityFirst considered URE's lack of cooperation as an aggravating factor in the penalty determination;[3]
7. the violations of RFC2014014015, RFC2014014410, RFC2014014012, and RFC2014014215 posed a minimal and not a serious or substantial risk to the reliability of the BPS. The violations of RFC2014014245, RFC2014014253, RFC2013013197, RFC2014013447, RFC2014013997, RFC2014014011, RFC2014014208, RFC2015015143, RFC2014014238, and RFC2014014239 posed a moderate and not a serious or substantial risk to the reliability of the BPS. The violations of RFC2014014014, RFC2014014251, RFC2014014252, RFC2014013623, RFC2014014207, RFC2015015300, RFC2014014209, RFC2013013198, RFC2014014211, RFC2014013998, RFC2014013626, RFC2014014262, RFC2014014114, RFC2014014216, RFC2014014257, RFC2014014240, RFC2014014241, RFC2014014241, RFC2014014013, RFC2015015302, RFC2014014242, and RFC2015015303 posed a serious risk to the reliability of the BPS; 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, in this instance, the penalty amount of one million seven hundred thousand dollars ($1,700,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

[3] Following the Compliance Audit, ReliabilityFirst experienced difficulty in obtaining substantive updates from URE regarding its mitigation progress. Despite numerous requests for updates following the Compliance Audit, ReliabilityFirst did not receive the majority of Mitigation Plans or substantive updates on mitigation progress until later than requested. URE also had more recent issues with delays in submitting and completing Mitigation Plans.

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 February 9, 2016 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 the assessed penalty of one million seven hundred thousand dollars ($1,700,000) 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.

[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:

Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-0682 Phone 216-503-9207 Facsimile bob.wargo@rfirst.org Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-0683 Phone 216-503-9207 Facsimile jason.blake@rfirst.org Deandra Williams-Lewis* Director of Enforcement ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-0689 Phone 216-503-9207 Facsimile deandra.williamslewis@rfirst.org	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel 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 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

Kristen M. Senk* Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-0669 Phone 216-503-9207 Facsimile kristen.senk@rfirst.org	Gizelle Wray* Associate Counsel, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3016 (202) 644-8099 – facsimile gizelle.wray@nerc.net *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.

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
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Gizelle Wray
Associate Counsel
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.kichline@nerc.net
gizelle.wray@nerc.net
(202) 400-3000
(202) 644-8099 – facsimile

cc: Unidentified Registered Entity
ReliabilityFirst Corporation