PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

August 27, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity 1 (URE1), Unidentified Registered Entity 2 (URE2), and Unidentified Registered Entity 3 (URE3), FERC Docket No. NP14-_-000

Dear Ms. Bose:

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

This Notice of Penalty is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and the URE Companies 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 URE Companies neither admit nor deny the violations, but have agreed to the assessed penalty of six hundred and

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

twenty-five thousand dollars ($625,000) and the non-monetary penalty of an additional Spot Check, 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 and Attachment A to the Settlement Agreement. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC2012010910	CIP-002-1	R2	High/ Severe	URE2	$625,000
RFC2012010911 NPCC2014013552	CIP-002-1	R3	High/ Severe	URE2	
RFC2012010912 NPCC2014013553	CIP-002-1	R4	Lower/ Severe	URE2	
RFC2013011925	CIP-003-1	R1; R1.3	Lower/ Severe	URE1	
RFC2014013690 NPCC2014013556				URE2	
RFC2014013691				URE3	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC2012010093	CIP-003-1	R4	Medium/ High	URE1	$625,000
RFC2012010086				URE2	
RFC2012010079				URE3	
RFC201100889	CIP-003-1	R5	Lower/ High	URE1	
RFC201100896				URE2	
RFC201100903				URE3	
RFC2012010302 NPCC2014013554	CIP-003-1	R6	Lower/ Severe	URE2	
RFC2013011966				URE3	
RFC2012010303 NPCC2014013550	CIP-004-1	R3	Medium/ Severe	URE2	
RFC2012011364	CIP-004-3a	R3	Medium/ High	URE1	
RFC2014013316				URE3	
RFC2012010094	CIP-004-1	R4	Lower/ Severe	URE1	
RFC2012010087 NPCC2014013549				URE2	
RFC2012010080				URE3	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC2012010924	CIP-005-1	R1	Medium/ Severe	URE1	$625,000
RFC2012010305 NPCC2014013440				URE2	
RFC2013011967				URE3	
RFC201100890	CIP-005-1	R2	Medium/ Severe	URE1	
RFC201100897 NPCC2014013551				URE2	
RFC201100904				URE3	
RFC201100891	CIP-005-1	R3	Medium/ Severe	URE1	
RFC201100898 NPCC2014013548				URE2	
RFC201100905				URE3	
RFC2012010311	CIP-005-1	R4	Medium/ Severe	URE1	
RFC2012010297 NPCC2014013541				URE2	
RFC2012010314				URE3	
RFC2012010310	CIP-005-1	R5	Lower/ Severe	URE1	
RFC2012010298 NPCC2014013534				URE2	
RFC2012010315				URE3	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC201100892	CIP-006-3c	R1	Medium/ Severe	URE1	$625,000
RFC201100899 NPCC2014013536				URE2	
RFC201100906				URE3	
RFC2014013708	CIP-006-2	R2; R2.2	Medium/ Severe	URE1	
RFC2014013709 NPCC2014013535				URE2	
RFC2014013703				URE3	
RFC201100893	CIP-006-3c	R6	Lower/ Severe	URE1	
RFC201100900				URE2	
RFC201100907				URE3	
RFC201100894	CIP-007-1	R1	Medium/ Severe	URE1	
RFC201100901 NPCC2014013546				URE2	
RFC201100908				URE3	
RFC201100895	CIP-007-1	R2	Medium/ Severe	URE1	
RFC201100902 NPCC2014013545				URE2	
RFC201100909				URE3	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC2012010095	CIP-007-1	R3	Lower/ Severe	URE1	$625,000
RFC2012010088 NPCC2014013544				URE2	
RFC2012010081				URE3	
RFC2012010096	CIP-007-1	R4	Medium/ Severe	URE1	
RFC2012010089				URE2	
RFC2012010082				URE3	
RFC2012010097	CIP-007-1	R5	Lower/ Severe	URE1	
RFC2012010090 NPCC2014013537				URE2	
RFC2012010083				URE3	
RFC2012010098	CIP-007-1	R6	Lower/ Severe	URE1	
RFC2012010091 NPCC2014013543				URE2	
RFC2012010084				URE3	
RFC2012010925	CIP-007-1	R7	Lower/ Severe	URE1	
RFC2012010921 NPCC2014013542				URE2	
RFC2013011968				URE3	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC2012010099	CIP-007-1	R8	Lower/ Severe	URE1	$625,000
RFC2012010092 NPCC2014013540				URE2	
RFC2012010085				URE3	
RFC2012010313	CIP-007-1	R9	Lower/ High	URE1	
RFC2012010301 NPCC2014013539				URE2	
RFC2012010317				URE3	
RFC2012010926	CIP-008-1	R1	Lower/ High	URE1	
RFC2012010907 NPCC2014013538				URE2	
RFC2013011970				URE3	
RFC2012010927	CIP-009-1	R1	Medium/ Severe	URE1	
RFC2012010908 NPCC2014013547				URE2	
RFC2013011971				URE3	

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

BACKGROUND

The Settlement Agreement that is the subject of this Notice of Penalty resolves 100 violations covering multiple instances of noncompliance with CIP Reliability Standards. The violations were discovered through a combination of Self-Reports and findings from three Compliance Audits (one for each of the three entities). As they are all subsidiaries of the same corporation and subject to many of the same processes and procedures, many of the facts and circumstances of the violations apply to URE1, URE2, and URE3.

The full scope of these violations required longer-term, more comprehensive mitigation. ReliabilityFirst worked closely with the URE Companies, conducting an assist visit to help the URE Companies develop thorough and complete mitigation. This also helped to ensure that, in the interim, the violations posed no serious risks to the reliability of the bulk power system (BPS).

After determining the full scope of the violations and the mitigation activities, ReliabilityFirst observed that the state of the URE Companies' mitigation activities and compliance had not progressed as quickly as expected considering the time they had been working together to resolve these violations. This factor, along with the other adjustment factors set forth in the Regional Entity's Basis for Penalty section below, formed the basis of the $625,000 monetary penalty associated with this Settlement Agreement.

No harm to the BPS is known to have occurred as a result of the violations described in this Notice of Penalty.

CIP-002-1 R2 (RFC2012010910)

ReliabilityFirst conducted a Compliance Audit of URE2 (URE2 Compliance Audit). During the URE2 Compliance Audit, URE2 did not provide evidence that it performed a power flow analysis when developing its list of Critical Assets, as required by its risk-based assessment methodology.

ReliabilityFirst determined that URE2 had a violation of CIP-002-1 R2 for failing to develop a list of its identified Critical Assets through an annual application of its risk-based assessment methodology.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE2 through when URE2 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE2 had a procedure that stated other criteria for the identification of Critical

Assets. Further, a power flow analysis is not required by CIP-002 R2 to identify Critical Assets, nor is it typically included in a registered entity's risk-based assessment methodology as a criterion for the identification of Critical Assets. URE2 mistakenly included the power flow analysis in its risk-based assessment methodology; it was intended to be a tool for third parties to confirm URE2's classification of assets.

URE2's Mitigation Plan to address this violation was submitted to ReliabilityFirst stating it had been completed.

URE2's Mitigation Plan required URE2 to modify its procedure to eliminate the requirement for power flow analysis.

URE2 certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-002-1 R3 (RFC2012010911, NPCC2014013552)

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to maintain documentation to demonstrate that it evaluated all Cyber Assets associated with a Critical Asset when developing its list of Critical Cyber Assets (CCAs). URE2 represented that it performed an annual review of its CCA list, but that its evidence was incomplete in part. During the URE2 Compliance Audit, URE2 presented CCA lists that did not list an effective date or accurately reflect existing CCAs essential to the operation of the Critical Assets. In addition, URE2's documentation of annual approval of the CCA lists did not associate the approval form with a specific CCA list.

ReliabilityFirst determined that URE2 had a violation of CIP-002-1 R3 for failing to develop its lists of CCAs using the lists of Critical Assets developed pursuant to Requirement R2.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE2 through when URE2 completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE2's failure to develop complete CCA lists with dates and other necessary information increased the possibility that URE2 would not identify and afford the protections of the CIP Standards to all CCAs. However, URE2 did perform an annual review of its documentation, although it did not retain strong evidence regarding such reviews. Therefore, ReliabilityFirst considered this violation to relate to a documentation error.

URE2's Mitigation Plan to address these violations was submitted to ReliabilityFirst stating it had been completed.

URE2's Mitigation Plan required URE2 to implement a change to require the approver to sign and date the actual CCA list reviewed in addition to the completion of any formally-assigned workflows.

URE2 certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-002-1 R4 (RFC2012010912, NPCC2014013553)

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to ensure that a senior manager or delegate approved the list of Critical Assets, the list of CCAs, and the risk-based assessment methodology on an annual basis. Specifically, URE2 did not provide any evidence of senior manager or delegate approval of the risk-based assessment methodology. Instead, the evidence did not indicate or identify the CCA list that the URE2 senior manager or delegate reviewed or approved. Further, URE2 did not associate its approval forms with specific Critical Asset lists. The evidence did not indicate or identify the Critical Asset list that the URE2 senior manager or delegate reviewed or approved.

ReliabilityFirst determined that URE2 had a violation of CIP-002-1 R4 for failing to ensure that a senior manager or delegate annually approve the list of Critical Assets, the list of CCAs, and the risk-based assessment methodology.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE2 through when URE2 completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Although it did not retain sufficient evidence, a senior manager or delegate did in fact perform an annual review of the list of Critical Assets, list of CCAs, and risk-based assessment methodology.

URE2's Mitigation Plan to address these violations was submitted to ReliabilityFirst stating it had been completed.

URE2's Mitigation Plan required URE2 to review and implement updates to its designation and delegation documents to identify any areas for improvement and incorporate more specific delegation information into the designating document.

URE2 certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-003-1 R1 (RFC2013011925, RFC2014013690, RFC2014013691, NPCC2014013556)

ReliabilityFirst conducted a Compliance Audit of URE1 (URE1 Compliance Audit). During the URE1 Compliance Audit, URE1 reported to ReliabilityFirst that the facts and circumstances described in its previously-submitted CIP-003-1 R4 Self-Report also involved a violation of CIP-003-1 R1.3. Specifically, URE1 did not ensure that the assigned senior manager conducted an annual review and approval of URE1's cybersecurity policy.

Subsequently, URE2 and URE3 submitted Self-Reports to ReliabilityFirst to the same effect.

ReliabilityFirst determined that the URE Companies had violations of CIP-003-1 R1.3 for failing to conduct an annual review and approval of the cybersecurity policy by the senior manager assigned pursuant to CIP-003 R2.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. While the URE Companies failed to retain strong evidence, the URE Companies did in fact perform annual reviews of their cybersecurity policies.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The URE Companies' Mitigation Plans required the URE Companies to:

1. review their cybersecurity policies and update the change logs;
2. enhance the documentation for annual reviews of the cybersecurity policies; and
3. use their processes to ensure completion of annual reviews.

URE1, URE2, and URE3 each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-003-1 R4 (RFC2012010079, RFC2012010086, RFC2012010093)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-003-1 R4 for failing to implement their CCA information protection programs. Specifically, the URE Companies failed to properly classify and protect information repositories that house CCA information. Additionally, the URE Companies failed to complete the annual assessments of the CCA information protection programs, document the results of such assessments, and implement remediation plans for potential issues in accordance with CIP-003-1 R4.3.

ReliabilityFirst determined that each of the URE Companies had violations of CIP-003-1 R4 for failing to implement its program to identify, classify, and protect information associated with CCAs, and for failing to assess annually adherence to its CCA information protection program, document the assessment results, and implement an action plan to remediate deficiencies.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure of the URE Companies to implement and document their programs to identify, classify, and protect information repositories that housed CCA information increased the possibility that the protections in place for protected CCA information would be decreased or eliminated.

However, the risk was mitigated by several factors. Although the URE Companies failed to classify appropriately certain files containing protected information, this information did reside in secure locations with access control mechanisms implemented. The URE Companies store their CCA information in repositories housed on their internal networks, which allow access to only those individuals housed on the URE Companies internal networks and bearing user access credentials. In most cases, shared drives and similar repositories that have department and/or team-level access restrictions housed these repositories. These access restrictions required specific approvals by a management-level official or higher in order to ensure the individuals who authorized the access were personnel in trusted supervisory roles and with requisite knowledge of the access need of the requested employee. In other instances, physical repositories (i.e., locked file cabinets) were located within an existing Physical Security Perimeter (PSP), which had physical protections and access restrictions.

Further, while the URE Companies failed to maintain adequate documentation of their annual reviews of the CCA information protection programs, the URE Companies did in fact perform these annual reviews.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The URE Companies' Mitigation Plans required the URE Companies to:

1. review their protected information to ensure it resides within a protected information repository;
2. develop revisions to their restricted information procedures and processes and train relevant staff on these revisions;
3. develop and implement a plan to assure proper classification in the first instance to minimize possibility of over classification of protected information; and
4. implement their annual reviews of their information protection programs.

URE1, URE2, and URE3 each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-003-1 R5 (RFC201100889, RFC201100896, RFC201100903)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they failed to implement their program for managing vendor access to protected CCA information. Specifically, the URE Companies did not verify that the external vendor personnel who could access protected CCA information during the course of their IT support functions met the requirements for training and personnel risk assessments (PRAs) prior to granting access to such information.

The URE Companies subsequently reported that they failed to classify properly information repositories that housed CCA information and subsequently failed to provide the repositories and the information within the repositories with the protections specified within their program for managing access to protected CCA information. URE2 properly classified its two repositories, but stored information that was not properly classified in those repositories. URE1 under-classified approximately 15% of its repositories, and URE3 under-classified approximately 25% of its repositories.

During the URE2 Compliance Audit, URE2 failed to provide evidence of an annual verification of personnel responsible for authorizing access to protected information or an annual review of the

access privileges to protected information to confirm that access privileges are correct and correspond with URE2's needs and appropriate personnel roles and responsibilities.

In addition, the URE Companies reported that they did not retain evidence of grandfathered users' need for access for a number of individuals with access to protected information. Therefore, the URE Companies failed to document that their access privileges were correct and that they corresponded with the URE Companies' needs and appropriate roles and responsibilities.

ReliabilityFirst determined that the URE Companies had violations of CIP-003-1 R5 for failing to implement their program for managing access to protected CCA information.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to implement their program for managing access to protected CCA information increased the possibility that protections in place for access to protected CCA information would be decreased.

However, ReliabilityFirst determined that the URE Companies implemented certain controls to provide security to their Critical Assets and CCAs. First, although the URE Companies failed to classify appropriately certain files containing protected information and provide the information with the protections specified in their programs, this information did reside in secure locations with access control mechanisms implemented. See the risk assessment for CIP-003-1 R4 (RFC2012010079, RFC2012010086, RFC2012010093) above. Second, the URE Companies subsequently verified that the external vendor personnel with access to protected CCA information completed the training and PRA requirements.

Third, the individuals without confirmed access privileges were initially granted access during their work on the NERC CIP compliance development team, which occurred prior to the mandatory and enforceable date of the Standard. Although the URE Companies' documentation was insufficient, all of these individuals were and are trusted users who have approved network access credentials.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The URE Companies' Mitigation Plans required the URE Companies to:

1. review their protected information to ensure that it resides within a protected information repository;
2. develop and communicate revisions to their restricted information policies and procedures;
3. review user PRA records, training records, access control lists, and user access privileges to protected information; and
4. review and verify their remaining CIP-003 R5 related procedures and remediate identified gaps.

URE1, URE2, and URE3 each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-003-1 R6 (RFC2012010302, RFC2013011966, NPCC2014013554)

URE2 submitted a Self-Report to ReliabilityFirst stating that it had a violation of CIP-003-1 R6 for failing to implement supporting configuration management activities to identify, control, and document all changes to a set of CCAs pursuant to its change control process. Specifically, URE2 failed to follow all of its change control processes for a set of computers and computer consoles classified as CCAs. ReliabilityFirst confirmed that these facts and circumstances constituted a violation during the URE2 Compliance Audit.

Subsequently, URE3 submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit, URE3 did not have sufficient evidence to demonstrate that it implemented supporting configuration management activities to identify, control, and document all changes to CCAs pursuant to its change control process.

ReliabilityFirst determined that URE2 and URE3 had violations of CIP-003-1 R6 for failing 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 their change control processes.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on URE2 and URE3 through when URE2 and URE3 completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure of URE2 and URE3 to identify, control,

and document all entity or vendor-related changes to CCA hardware or software could have increased the possibility of system outages or downtime associated with unauthorized and/or undocumented changes. However, URE2 and URE3 provided certain security management controls to protect CCAs. Specifically, while some CCAs were not subject to all steps within their change control processes, all assets were subject to some aspects of the processes. Further, all assets at all times resided within the defense-in-depth perimeters, which included layers of firewall protection and monitoring within the Electronic Security Perimeters (ESPs) and PSPs.

URE2's Mitigation Plan and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required URE2 and URE3 to:

1. reinforce the proper implementation of existing change control processes to appropriate personnel;
2. ensure that previously excluded CCAs were subjected to the change control procedures;
3. revise the change control process document; and
4. perform a quality assessment with an action plan to address lessons learned from the quality assessment with the appropriate personnel.

URE2 and URE3 each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-004-1 R3 (RFC2012010303 and NPCC2014013550) and CIP-004-3a R3 (RFC2012011364 and RFC2014013316)

URE2 submitted a Self-Report to ReliabilityFirst stating that it had a violation of CIP-004-1 R3 for failing to update the PRA for one contractor at least every seven years after the initial PRA, and for failing to revoke this contractor's access between the expiration and subsequent renewal of the contractor's PRA. Additionally, during the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to include a provision requiring URE2 to update each PRA for cause in its documented PRA program.

Subsequently, URE3 submitted a Self-Report to ReliabilityFirst stating that it failed to update the PRA for five employees at least every seven years after the initial PRA.

URE1 later submitted a Self-Report to ReliabilityFirst stating it failed to update the PRAs for six employees every seven years after the initial PRA.

URE2 later reported that it failed to update the PRAs for four employees in addition to the previously-identified contractor.

ReliabilityFirst determined that URE2 had a violation of CIP-004-1 R3 for failing to update the PRA for one contractor and four employees at least every seven years. ReliabilityFirst determined that URE3 had a violation of CIP-004-3a R3 for failing to update the PRA for five employees. ReliabilityFirst determined that URE1 violated CIP-004-3a R3 for failing to update the PRA for six employees.

ReliabilityFirst determined the duration of URE2's violation to be from the date the Standard became mandatory and enforceable on URE2 through when URE2 completed its Mitigation Plan. ReliabilityFirst determined the duration of URE3's violation to be from the date of URE3's earliest identified noncompliance through when URE3 completed its Mitigation Plan. ReliabilityFirst determined the duration of URE1's violation to be from the date of URE1's earliest identified noncompliance through when URE1 completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. For the URE2 violation, the contractor's PRA was late by 31 days, and URE2's existing access monitoring processes immediately identified and escalated the issue. The contractor was a trusted vendor who had a previously-valid PRA, and the renewed PRA indicated no PRA-disqualifying factors. Further, the contractor was a member of a well-known and widely-used vendor managed security services staff. URE2 had external audit results that demonstrated the effective design and operation of the vendor's controls. Lastly, URE2 required PRAs for all contractors and employees who needed access to CCAs, even though its documentation was lacking. URE2 has experienced no instances of "for cause" situations since the date of mandatory compliance.

In relation to the URE Companies' failures to update employee PRAs in a timely manner, once identified, the URE Companies immediately removed the access for the employees with expired PRAs and subsequently updated each PRA. The URE Companies instituted manual processes to ensure timely PRAs until they could remedy the issues they experienced with their automated system that led to these violations. Further, the URE Companies used their monitoring and detective controls and verified that these individuals did not conduct inappropriate activities during the time their PRAs were expired.

URE3's Mitigation Plan and URE1's Mitigation Plan to address their violations were submitted to ReliabilityFirst stating they had been completed.

The Mitigation Plans required URE3 and URE1 to:

1. remove access for all employees with expired PRAs;

2. develop additional guidance for personnel entering PRA data into the human resources systems;
3. reprogram their systems to prevent future transposing of PRA data;
4. correct the PRA data entry errors for the individuals with access; and
5. train personnel on the proper insertion of PRA data into their systems.

URE2's Mitigation Plan to address its violation was submitted to ReliabilityFirst stating it had been completed.

In addition to completing the steps also undertaken by URE3 and URE1, URE2's Mitigation Plan required URE2 to:

1. renew the PRA for the contractor;
2. update its PRA procedure to include the renewal of PRAs for cause; and
3. replace vendor-managed firewalls with URE Company-managed firewalls to ensure appropriate management of access control and PRA processes for the affected assets.

The URE Companies each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-004-1 R4 (RFC2012010080, RFC2012010087, RFC2012010094, NPCC2014013549)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-004-1 R4 for failing to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs. Specifically, the URE Companies failed to include all of their information technology (IT) administrators on their list of personnel with authorized access to CCAs because these individuals gained access through their addition to groups that gave them access privileges, instead of through the standard access review and approval process.

During the URE2 Compliance Audit, URE2 failed to provide evidence demonstrating that it conducted a quarterly review of the lists of its personnel with access to CCAs, nor was it able to provide evidence that it updated the lists within seven calendar days of any change.

URE3 subsequently reported that it failed to remove an individual from its list of individuals with physical access to CCAs until five days after removal was required. URE3 discovered this issue during its quarterly review of the lists of personnel with access to CCAs.

During the URE1 Compliance Audit, URE1 failed to provide evidence demonstrating that it properly maintained the list of personnel with authorized cyber or authorized unescorted physical access to CCAs. Instead, URE1 provided an access list which did not include specific electronic access rights for all personnel with cyber access. Following the URE1 Compliance Audit, URE3 reported that it also failed to maintain sufficient evidence demonstrating the specific access rights of personnel with access to CCAs.

ReliabilityFirst determined that the URE Companies had violations of CIP-004-1 for failing to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The URE Companies trained and conducted PRAs on all IT administrators and granted each with access through local area network IDs and password credentials. In addition, while the access lists did not contain all of the required information, the URE Companies did maintain access lists with some of the required information. Further, the URE Companies implemented authorization criteria for all individuals accessing CCAs, including PRA and training requirements, and record basic access information. Lastly, URE3 retrieved the access badge of the individual who no longer required physical access to CCAs. Therefore, while the individual remained on the access list, the individual did not have the ability to access the area.

URE1's Mitigation Plan and URE3's Mitigation Plan to address their violations were submitted to ReliabilityFirst. URE2's Mitigation Plan to address its violation was submitted to ReliabilityFirst stating it had been completed.

The Mitigation Plans required the URE Companies to:

1. define access group ownership;
2. add appropriate individuals to the asset lists;
3. perform a quality assessment review of existing practices for maintaining authorized access lists; and
4. implement enhancements to their existing processes for maintaining authorized access lists.

The URE Companies each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-005-1 R1 (RFC2012010305, RFC2012010924, RFC2013011967, NPCC2014013440)

URE2 submitted a Self-Report to ReliabilityFirst stating that it had a violation of CIP-005-1 R1 for failing to identify and document two devices that would permit access up to the ESP. Subsequently, during the URE2 Compliance Audit, ReliabilityFirst discovered additional instances of noncompliance. Specifically, URE2 failed to: (i) identify an access point to its ESP within its ESP diagram; (ii) maintain sufficient evidence to demonstrate that it afforded any of the protective measures specified in CIP-005-1 R1.5 to its firewall management device (a Cyber Asset used in the access control and monitoring of the ESPs), and (iii) reflect revision history or version maintenance on its ESP diagrams.

Subsequently, URE1 submitted a Self-Report to ReliabilityFirst stating that it could not establish that it had identified all access points to the ESPs and could not establish that it afforded the protective measures specified in CIP-005-1 R1.5 to all Cyber Assets used in the access control and monitoring of the ESPs. During the URE1 Compliance Audit, ReliabilityFirst determined that URE1 also failed to ensure and document that every CCA resides within an ESP and failed to identify and document all ESPs (R1 and R1.6). Further, ReliabilityFirst identified that, in several of the instances self-reported by URE1 involving URE1's failure to identify access points, URE1 failed to consider communication links terminating at end points within defined ESPs as access points to the ESPs (R1.3).

Later, URE3 submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit and the URE1 Compliance Audit, it did not have sufficient evidence to demonstrate compliance with CIP-005-1 R1. Specifically, URE3 could not demonstrate that it: (i) identified access points to the ESP; (ii) identified and protected non-critical Cyber Assets within a defined ESP; (iii) afforded the protective measures specified in CIP-005-1 R1.5 to Cyber Assets used in the access control and monitoring of the ESPs; or (iv) maintained documentation of all electronic access points to the ESPs.

Subsequently, URE2 reported that it did not have sufficient evidence to demonstrate that it provided all CIP-005 protections to a set of printers within an ESP, as required by CIP-005-1 R1.4.

ReliabilityFirst determined that the URE Companies had violations of CIP-005-1 R1 for failing to identify access points to the ESP, afford the protective measures specified in CIP-005-1 R1.5 to Cyber Assets used in the access control and monitoring of the ESP, maintain documentation of the ESP and all electronic access points to the ESP, and identify and protect non-critical Cyber Assets within a defined ESP.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies until mitigated.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failures to identify all access points to the ESPs and provide them with the required protections increased the possibility of unauthorized electronic access to CCAs and non-critical Cyber Assets, potentially resulting in system misuse or compromise.

However, the URE Companies did implement measures to provide protections to ESPs, access points to ESPs, Cyber Assets used in the access control and monitoring of the ESPs, and CCAs. The URE Companies provide all assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy.

In addition, although the affected devices may not have been subject to certain CIP-005-1 R1 required procedures, they were subject to general access processing and change control requirements, which provide security for the system by limiting unauthorized access and protect against unexpected or unauthorized changes based on existing processes.

With respect to URE1's violation, URE1 applied CIP-005-1 R1 requirements, with the exception of documenting the access points on its ESP diagram. URE1 initially classified two types of access points only as CCAs instead of CCAs and electronic access points; as CCAs, they were afforded all CIP protections. Further, these access points do not allow interactive access into the device or the ESP.

With respect to URE3's violation, URE3 misclassified access points to the ESP as either CCAs or other types of assets requiring protection, applying applicable protections to those devices.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to:

1. revise existing documentation and develop additional documentation and guidance for the classification of electronic access points to the ESP, non-critical Cyber Assets, Cyber Assets used the access control and monitoring of the ESPs, and protected Cyber Assets;
2. use the revised and newly-added documentation to identify appropriate assets and update all ESP diagrams;

3. perform an analysis of the identified assets for required CIP controls based on their classification and implement the appropriate CIP protections on each asset; and
4. provide appropriate communication and training on these changes to personnel.

CIP-005-1 R2 (RFC201100890, RFC201100897, RFC201100904, NPCC2014013551)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-005-1 R2 for failing to ensure the authenticity of an accessing party in situations where they had enabled external interactive access into the ESP and for failing to document the technical and procedural mechanisms for control of electronic access at all electronic access points to the ESP.

The URE Companies permitted external vendors performing IT support functions to use a single generic user identification. As a result, the URE Companies were unable to determine the identity of a specific person accessing the ESP and consequently could not ensure the authenticity of the accessing party. Additionally, the URE Companies permitted external interactive access to the ESPs through the use of a reporting tool. Once a user installed the tool, it could access the ESP. The URE Companies did not implement authentication controls on this tool. In one instance, a user accessing the application had access to an information repository hosted on a CCA, but the URE Companies had not first ensured the authenticity of this individual.

The URE Companies also did not implement their technical and procedural mechanisms for control of remote access to the supervisory control and data acquisition (SCADA) system. The URE Companies have a process for control of electronic access at electronic access points to the ESP, but this process was not implemented for remote access to the SCADA system. Specifically, the URE Companies did not document the continuous monitoring of a vendor performing SCADA IT work as specified within the URE Companies' organizational processes and technical and procedural mechanisms for control of electronic access.

Subsequently, the URE Companies reported that IT administrators were able to bypass the URE Companies' controls and gain access to CCAs within an ESP through the use of an active directory authentication control. URE2 also self-reported that it failed to identify and document two devices that would permit access up to the ESP.

During the URE2 Compliance Audit, ReliabilityFirst determined that a previous Self-Report for a violation of CIP-007-1 R2 also indicated noncompliance with CIP-005-1 R2. Specifically, URE2 did not document that it only enables ports and services required for operations and monitoring as required by CIP-005-1 R2.2. URE2 stated that it does not perform firewall rule set reviews for validity once a firewall rule is approved and implemented.

During the URE1 Compliance Audit, URE1 stated that its previously self-reported CIP-007-1 R2 violation also indicated a violation of CIP-005-1 R2. Specifically, URE1 did not document that it only enables ports and services required for operations as required by CIP-005-1 R2.2.

ReliabilityFirst determined that the URE Companies had violations of CIP-005-1 R2 for failing to document and implement organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESPs.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies until mitigated.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the inconsistent application of organizational processes and technical and procedural mechanisms for controlling electronic access at all electronic access points to the ESP could have left access points, and therefore the ESP, exposed to unauthorized access and vulnerable to cyber intrusion.

However, the URE Companies implemented measures to provide protection to Cyber Assets within the ESP, as well as to access points to the ESP. First, the vendor personnel using the generic identification were required to authenticate to the URE Companies' environments before accessing electronic access points to the ESP. The URE Companies monitored the vendors' work as it occurred. Further, all personnel assigned to the generic user identification had completed PRAs and CIP training. Second, access to the reporting tool was limited to those individuals with authorization to access the corporate domain, the application itself, or a link to the application, and access to the tool from within the corporate network.

Third, while IT administrators were able to access CCAs within an ESP through the active directory authentication control, only the local IT administrators were able to use this access, and each of these users had network access credentials and received training and PRAs.

Fourth, while the URE Companies' documentation was insufficient, the URE Companies did secure their SCADA networks and had implemented remote access processes and controls.

Fifth, the URE Companies provide all assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by these violations.

Lastly, in relation to the ports and services issue, the URE2 and URE1 violations related to the proper documentation of baselining of open ports and services accompanied by the operational and business need for those ports and services to be open. The URE Companies followed a formal process for review, approval, and implementation of firewall rules. The firewalls deny access by default, and dial-up access to or within the ESP is not permitted by policy. The URE Companies also perform routine vulnerability assessments for the affected devices, although their documentation was lacking appropriate details to establish compliance in certain instances.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to:

1. revise and add documentation and guidance for the classification of electronic access points to the ESP, non-critical Cyber Assets, Cyber Assets used in the access control and monitoring of the ESPs, and protected Cyber Assets;
2. use the revised and newly-added documentation to identify appropriate assets and update all ESP diagrams;
3. perform an analysis of the identified assets for required CIP controls based on their classification and implement the appropriate CIP protections on each asset;
4. remove the reporting tool application from the ESP;
5. implement updates to existing processes, technical mechanisms, and current procedural documentation;
6. review prior baselining of ports and services;
7. develop a new process for the baselining of ports and services;
8. conduct a baselining of ports and services for each Cyber Asset; and
9. provide appropriate communication and training on these changes to personnel.

CIP-005-1 R3 (RFC201100891, RFC201100898, RFC201100905, NPCC2014013548)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-005-1 R3 for failing to implement an electronic or manual process for monitoring and logging access points to the ESPs at all times. Specifically, the URE Companies allowed external vendors to remotely access CCAs through the use of one generic identification for multiple individuals, while being monitored by an employee. More than one person was able to use the same identification; as a result,

the URE Companies could not authenticate or log the specific person accessing a CCA at a given access point.

Subsequently, the URE Companies self-reported that they failed to implement a process for monitoring and logging when IT administrators were able to access ESPs through an active directory authentication tool which did not monitor and log access. URE2 also reported that it failed to implement and document processes at two devices identified as CCAs with dial-up accessibility.

The URE Companies also reported that, in the process of implementing mitigating activities to address their noncompliance with CIP-005 R3, they discovered that they were not subjecting certain firewall devices to existing logging, monitoring, and alerting processes. Since the logs did not exist, the URE Companies could not perform manual reviews of logs.

ReliabilityFirst determined that the URE Companies had violations of CIP-005-1 R3 for failing to implement and document an electronic or manual process for monitoring and logging access at access points to the ESP at all times.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failures to implement processes for monitoring and logging access at access points to the ESPs provided the opportunity for individuals to access their ESPs while leaving no record of the intrusion. This increased the possibility that the URE Companies would be unable to prevent or track intrusions that could result in harm to the integrity of the CCAs within the ESPs.

However, the URE Companies did implement measures to detect and alert for unauthorized access to their ESPs and to protect Cyber Assets within the ESP as well as access points to the ESP.

First, the vendor personnel using the generic identification were required to authenticate to the URE Companies' environments before accessing electronic access points to the ESP. The URE Companies monitored the vendors' work as it occurred. Further, all personnel assigned to the generic user identification had completed PRAs and CIP training. Second, while IT administrators were able to access CCAs within an ESP through the active directory authentication control, only the local IT administrators were able to use this access, and each of these users had network access credentials and received training and PRAs. Third, while the URE Companies' documentation was insufficient, the

URE Companies did secure their SCADA networks and had implemented remote access processes and controls.

Fourth, URE2's ESP firewalls have a deny-by-default policy. URE2 requires that access be requested through its firewall change request process. Access, if approved, is granted through the firewalls based on source IP address, destination IP address, and destination ports as requested. Personnel verify that users requiring interactive access into the ESP have a background check and CIP training before granting access.

Lastly, the URE Companies provide all assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by these violations.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to:

1. revise active directory group ownership and add new groups to assets where necessary;
2. document the practices for electronic remote access into the ESP;
3. implement updates to existing processes, technical mechanisms, and current procedural documentation; and
4. perform quality assurance reviews of account logging and monitoring on checkpoint firewalls to confirm authentication methods and their ability to log and monitor activity appropriately.

CIP-005-1 R4 (RFC2012010297, RFC2012010311, RFC2012010314, NPCC2014013541)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they each had violations of CIP-005-1 R4 for failing to conduct a review to verify that only ports and services required for operations at the access points are enabled during their annual CVA of the electronic access points to the ESPs. Additionally, the URE Companies failed to maintain documentation demonstrating that their annual CVAs include a document identifying the vulnerability assessment process, the discovery of all access points to the ESP, a review of controls for default accounts, passwords, and network management community strings, and documentation of the results of the assessment, the action plan

to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

In addition, during the URE2 Compliance Audit, URE2 failed to provide evidence to demonstrate that a vulnerability assessment plan existed, as required by its CVA process. ReliabilityFirst also discovered that URE2's CVA process does not require URE2 to document the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, or the execution status of that action plan. Finally, URE2 failed to submit evidence to demonstrate compliance with any of the remaining sub requirements of CIP-005-1 R4.

ReliabilityFirst determined that the URE Companies each had violations of CIP-005-1 R4 for failing to maintain documentation that they performed an annual CVA of the electronic access points to the ESPs that included each of the required provisions.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to conduct compliant CVAs increased the possibility that the URE Companies would be unaware of discoverable and preventable cyber vulnerabilities, and that an individual could exploit these vulnerabilities to gain unauthorized access to CCAs within the ESPs.

However, the URE Companies did implement protections to reduce the risk of unauthorized access to the ESPs. Although the URE Companies did not document the implementation of CVA requirements as defined in CIP-005-1 R4, they were conducting vulnerability scanning through a vulnerability scanning program. In addition, the URE Companies provide all cyber assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by these violations.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to:

1. review prior baselining and develop a new process for the baselining of ports and services;
2. conduct a baselining of ports and services for each Cyber Asset;

3. revise their documented CVAs and annual review processes to develop CIP-specific processes and supporting documentation for CVAs; and
4. perform an annual review of in-scope documentation and an annual CVA.

CIP-005-1 R5 (RFC2012010298, RFC2012010310, RFC2012010315, NPCC2014013534)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-005-1 R5 for failing to annually review, update, and maintain all documentation to support compliance with the requirements of Reliability Standard CIP-005. The reviews of program documents were not completed in a timely manner.

During the URE2 Compliance Audit, ReliabilityFirst also discovered that the URE2 ESP diagrams did not reflect revision history or version maintenance to demonstrate that URE2 maintained the ESP diagrams as required.

ReliabilityFirst determined that the URE Companies had violations of CIP-005-1 R5 for failing to annually review, update, and maintain all documentation to support compliance with the requirements of CIP-005.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The URE Companies have documented processes requiring the annual review and approval of CIP-related documentation. These violations reflected documentation deficiencies related to the URE Companies' workflow processes and the inability to produce evidence of annual task completion.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to update existing processes, technical mechanisms, and current procedural documentation, and perform an annual review of in-scope documentation.[4]

[4] In addition, as part of the overall mitigation work, the URE Companies have made significant improvements to the annual review and documentation processes.

CIP-006-3c R1 (RFC201100892, RFC201100899, RFC201100906, NPCC2014013536)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-006-3c R1 for failing to implement their visitor control programs documented in their physical security plans. Specifically, the URE Companies reviewed instances where employees and contractors without authorized unescorted access to PSPs entered the PSPs without an escort.

During the URE2 Compliance Audit, URE2 failed to provide sufficient evidence to demonstrate that the physical security plan is reviewed at least annually and approved by the senior manager or delegate. ReliabilityFirst also discovered that, while URE2 identified all physical access points through each PSP and measures to control entry at those access points, URE2 did not include this information within its physical security plan. Further, ReliabilityFirst discovered that URE2 failed to ensure that all Cyber Assets within an ESP also reside within a defined PSP, when a completely enclosed six-wall border could not be established for Ethernet network cabling for CCAs. No Technical Feasibility Exception (TFE) was submitted.

ReliabilityFirst determined that the URE Companies had violations of CIP-006-3c R1 for failing to implement a physical security plan that addresses a visitor control program mandating escorted access of visitors within the PSP, and for failing to document, implement, and maintain a physical security plan, approved by a senior manager or delegate, that addresses the sub-requirements of the Standard.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to document, implement, and maintain a physical security plan addressing the sub-requirements of R1 increased the possibility that an individual could physically access, misuse, or compromise Cyber Assets that were not protected. Further, individuals without proper authorization and proper escort gained access to PSPs.

However, the risk was mitigated by several factors. In each instance related to the visitor access program, the issues involved existing employees or contractors, many of whom were in the process of being authorized. None of the instances involved a malicious attempt to access a restricted area. Further, the URE Companies provided protections to control a visitor's access to PSPs. These protections included door alarms and security notifications, which were working during the period of the violations. In addition, each PSP area was monitored by security personnel through cameras and alarm systems.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address their violations were submitted to ReliabilityFirst stating they had been completed.

The Mitigation Plans required the URE Companies to:

1. develop guidance for visitor access;
2. update their visitor access procedures and associated training modules;
3. develop a formal security guidance document for minimal security controls for restricted areas;
4. revise signage practices for restricted areas;
5. assess physical access control equipment at each restricted area;
6. develop a guidance document that provides standard inspection requirements to be used at all restricted areas; and
7. train relevant personnel on these changes.

In addition, URE2's Mitigation Plan required URE2 to:

1. move assets housed in the areas identified in the URE2 Compliance Audit findings; and
2. decommission those areas and update its PSP diagrams to reflect the decommissioning.

The URE Companies certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-006-2 R2.2 (RFC2014013703, RFC2014013708, RFC2014013709, NPCC2014013535)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-006-2 R2.2 for failing to afford the protective measures required in the Standard to some newly-identified physical access control system (PACS) devices, which are devices that authorize and log access to the PSPs.

ReliabilityFirst determined that the URE Companies had violations of CIP-006-2 R2.2 for failing to afford the protective measures specified in the Standard to Cyber Assets that authorize and/or log access to the PSPs.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies until mitigated.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to provide the protections of CIP-006 R2.2 to the PACS devices increased the possibility that unknown or unauthorized individuals could physically access CCAs, resulting in the misuse or compromise of the CCAs.

However, the URE Companies did provide some protections to limit the risk posed to their PACS devices. The newly-identified PACS devices are located inside a PSP and further locked inside cabinets therein. Electronic access to those devices is limited by default to only those individuals that had access to other PACS devices that the URE Companies protected in accordance with CIP-006-2 R2.2. The URE Companies did not identify any instances of deliberate attempts to circumvent physical access controls. Further, the URE Companies provide all assets a baseline level of protections based on the URE Companies' corporate policies and procedures and defense-in-depth security strategy. The PACS devices were provided protections such as access processing and change control requirements.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to:

1. analyze the CIP controls required for the newly-identified PACS devices and implement the controls on the devices;
2. ensure personnel with access to the devices had current PRAs and training, and retrain the personnel on the change made to the PACS devices;
3. assess the need for TFEs on technically-infeasible controls;
4. design and implement the controls required for the PACS devices; and
5. perform a quality assurance assessment to verify the controls for these devices are operating as intended.

CIP-006-3c R6 (RFC201100893, RFC201100900, RFC201100907)

The URE Companies submitted Self-Reports of CIP-006-3c to ReliabilityFirst stating that they had violations of CIP-006-3c R6 for failing to implement technical and procedural mechanisms for logging physical entry at all access points to the PSPs. Specifically, the URE Companies reviewed incidents where personnel entered restricted areas, which were defined PSPs, without appropriate access rights

or an escort. Additionally, URE3 identified one instance of intermittent door lock failures to a PSP door.

ReliabilityFirst determined that the URE Companies had violations of CIP-006-3c R6 for failing to implement and document the technical and procedural mechanisms for logging physical entry at all access points to the PSPs in accordance with the Standard.

ReliabilityFirst determined the duration of the violations to be from the date of each of the URE Companies' earliest identified noncompliance through when each of the URE Companies completed the mitigating activities necessary to remedy its violation.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to implement and document the technical and procedural mechanisms for logging physical entries at their PSPs increased the possibility that unauthorized individuals could gain physical access to Cyber Assets.

However, the instances where individuals gained access involved existing employees or contractors who were either in the process of being authorized and believed themselves already to have proper authorization or who would have been escorted had they understood the area to be a restricted area. None of the instances involved a malicious attempt to access a restricted area. Additionally, all door alarms and security notifications were functional at the time of the violations, and each area was monitored by security personnel through the use of cameras and alarm systems.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address their violations were submitted to ReliabilityFirst stating they had been completed.

The Mitigation Plans required the URE Companies to:

1. develop guidance for visitor access;
2. update their visitor access procedure and associated training modules;
3. develop a formal security guidance document for establishing minimal security controls for restricted areas;
4. revise signage practices for restricted areas;
5. assess physical access control equipment at each restricted area;
6. develop a guidance document that provides standard inspection requirements to be used at all restricted areas; and

7. train relevant personnel on the changes.

URE1, URE2, and URE3 each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-007-1 R1 (RFC201100894, RFC201100901, RFC201100908, NPCC2014013546)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R1 for failing to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls. While the URE Companies reported that they conducted significant testing on changes, the URE Companies could not establish that this testing ensured that changes did not adversely impact cybersecurity controls.

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

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The URE Companies make very few significant changes to CCAs on an annual basis. Further, the URE Companies completed all changes in accordance with a change control process that includes risk-based testing, and they test all changes in a quality assurance environment before they implement the change on the CCA. All Cyber Assets within the ESP resided within defense-in-depth perimeters, including layers of firewall protection and monitoring for events within the ESPs and PSPs. Additionally, some Cyber Assets are not connected to the internet.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plan required the URE Companies to:

1. revise their definition of a significant change;
2. update their test procedures;
3. develop a checklist, by asset type, for testing cybersecurity controls when a significant change occurs;

4. train relevant personnel on the revised checklist and processes;
5. perform an assessment to determine whether the revised processes and checklists were followed during a significant change; and
6. develop recommended actions based on the assessment of the implementation of the revised processes and procedures.

CIP-007-1 R2 (RFC201100895, RFC201100902, RFC201100909, and NPCC2014013545)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R2 for failing to establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled. Specifically, the URE Companies reported that they conducted testing on Cyber Assets and determined that they were unable to confirm that only ports and services required for normal and emergency operations were enabled.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R2 for failing to establish and document 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 the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure increased the possibility that unauthorized network traffic could infiltrate the ESP through ports and services that are not necessary for normal or emergency operations but nevertheless remain enabled.

However, the URE Companies provided some protections to their systems to reduce the risk of vulnerabilities. First, the URE Companies provided periodic vulnerability scans to identify open ports and services and then evaluated and managed any issues through the scanning process. Second, the URE Companies used vulnerability scanning to identify vulnerabilities within the ESP that, when closed through vulnerability assessment remediation, effectively keep the systems within the ESP more hardened related to patching, closing unneeded or vulnerable services, and upgrading unsupported or vulnerable systems. Third, the URE Companies reviewed all ESP and CCA ports during initial implementation. Fourth, the URE Companies encompass ESPs with additional electronic perimeters, separating the real-time networks from the corporate network and the internet. These electronic

perimeters are monitored by an intrusion detection system (IDS). Lastly, all Windows assets have antivirus software installed.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. review prior baselining of ports and services;
2. develop a new process for the baselining of ports and services; and
3. conduct a baselining of ports and services for each Cyber Asset.

CIP-007-1 R3 (RFC2012010081, RFC2012010088, RFC2012010095, NPCC2014013544)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R3. Specifically, the URE Companies failed to follow the corporate patch management program for certain devices. The URE Companies also reported that they were unable to demonstrate that they assessed certain patches for applicability within 30 calendar days of availability. URE1 also reported that for one Cyber Asset, it was not technically feasible to install the patch, but URE1 failed to document the compensating measures applied to mitigate risk exposure or acceptance of the risk.

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to demonstrate that it assessed patches for applicability for certain devices and applications within 30 calendar days of availability.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R3 for failing to document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability. In addition, ReliabilityFirst determined that URE1 had a violation of CIP-007-1 R3 for failing to document compensating measures applied to mitigate risk exposure or an acceptance of the risk in one instance where a patch was not installed.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to follow their patch management programs increased the possibility that unauthorized network traffic could infiltrate the

ESP or that a malicious individual could exploit known vulnerabilities. However, several factors mitigated the risk during the duration of the violations.

All Cyber Assets within the URE Companies' ESPs resided within defense-in-depth perimeters, including layers of firewall protection and monitoring for events within the ESPs and PSPs. Some Cyber Assets are not connected to the internet.

URE1 was performing patch assessment and regular quarterly patching on a certain set of operating system assets throughout the compliance period. Prior to applying patches to all production assets, URE1 first applies patches to non-production assets that are not CCAs and which are segregated from the critical production assets in a quality assurance system environment. URE1 then performs functional and cybersecurity control testing and approval cycles. After this step, it then applies patches to lower-risk production assets before applying the patches to all production assets.

The URE Companies began regularly reviewing and implementing patches for most key elements, such as operating systems and crucial SCADA applications, during the compliance period.

URE2 began actively patching its remote terminal unit platforms and certain operating system units during the compliance period. Similar to URE1, URE2 first performs patching against non-production assets.

URE1 began actively monitoring, evaluating, and patching other key systems during the compliance period.

URE3 has performed assessments of released patches every 30 days beginning during the compliance period.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. update their patch management program, management model documents, and TFE filings;
2. determine which software should be subject to patch management processes;
3. design processes to monitor the release of vendor patches;
4. develop a process for alerting responsible personnel when vendor patches are released;

5. train appropriate personnel on implemented processes to ensure monitoring and patch reviews are occurring as expected; and
6. implement any remaining corrective actions based on the results of the assessments.

CIP-007-1 R4 (RFC2012010082, RFC2012010089, RFC2012010096)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R4. Specifically, the URE Companies failed to implement their processes for implementing antivirus and malware updates, including the requirements within those processes that mandate the testing and installation of signature files. In certain instances, the URE Companies encountered technical issues with the server's operating system, which was not able to support certain automatic updates. In those cases, the URE Companies did not document compensating measures applied to mitigate risk exposure or an acceptance of the risk.

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 did not install antivirus and malware prevention tools on a different server. ReliabilityFirst also discovered that URE2's process documentation did not address the testing of antivirus signatures for two sets of devices which are Cyber Assets within an ESP.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R4 for failing to document and implement antivirus software and other malware prevention tools on all Cyber Assets within the ESPs and by failing to implement a process for the update of antivirus and malware prevention signatures.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to ensure that all required devices implemented antivirus software and had updated signature files in place increased the possibility that malware could be introduced, exposed, and propagated on Cyber Assets within the ESP.

However, several factors mitigated the risk. First, the URE Companies used IDS to monitor all network traffic and compare aggregate traffic against known malicious signatures. All of the URE Companies' Cyber Assets are housed deep within the network infrastructure, which is isolated from typical

malware attack vectors. Email clients were not installed on these Cyber Assets, and the Cyber Assets did not have access to the internet.

In addition, the URE Companies provide all Cyber Assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by these violations.

Lastly, each instance of noncompliance with CIP-007-1 R4 was limited in scope.[5] These issues related to the URE Companies' failures to test signature files due to vendor errors in testing, apply compensating measures for technically infeasible malware application, and install antivirus and malware software on a single device inside an ESP that was not a CCA.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. perform a quality assurance review and assessment of existing antivirus and malware operations to identify compliance gaps;
2. assess their devices for necessary TFE filings;
3. implement technical solutions necessary to ensure compliance with the Standard; and
4. assess devices again to verify compliance.

CIP-007-1 R5 (RFC2012010083, RFC2012010090, RFC2012010097, NPCC2014013537)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R5. Specifically, the URE Companies failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

The URE Companies granted certain IT administrators access to Cyber Assets through authentication groups, which gave them access outside of the required approval process. The URE Companies also failed to require password changes for certain firewalls, routers, and switches on the 90-day interval required by their own processes. The URE Companies also failed to review user accounts to verify that access privileges are in accordance with CIP-003 R5 and CIP-004 R4 on an annual basis; several of these

[5] ReliabilityFirst considered the aggregate effect of each of these violations to pose a moderate risk to the reliability of the BPS, but considered each individual instance to be limited in scope.

reviews were completed late. The URE Companies reported that they were also in violation of CIP-007-1 R5.2, when they assigned generic administrator accounts to IT support personnel, but failed to authenticate specific individuals on login. The URE Companies also failed to authorize formally access to shared accounts in certain instances. Lastly, the URE Companies reported that they failed to enforce password complexity and frequency changes for certain Cyber Assets.

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 also failed to generate logs to create historic audit trails of individual user access activity for a minimum of 90 days for sampled devices and Windows platforms. URE2 failed to demonstrate that it implemented an annual review of user accounts to verify access privileges in accordance with CIP-007-1 R5.1.3. Lastly, ReliabilityFirst discovered that URE2 failed to have a policy for managing the use of shared accounts that includes a provision requiring an audit trail of the account use and steps for securing the account in the event of personnel changes, as required by CIP-007-1 R5.2.3.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R5 for failing to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failures to implement technical and procedural controls increased the possibility of unauthorized system access, potentially resulting in system misuse or compromise.

However, several factors mitigated the risk. First, each of the IT administrators had received training and PRAs and had approved network access credentials. Second, the URE Companies required the IT support personnel using the generic user identification to first authenticate to the corporate environment. All personnel had PRAs and CIP training, and the URE Companies monitored their work as it occurred.

Third, the URE Companies were performing some annual reviews and properly managing user account privileges, although these reviews did not meet all the requirements of CIP-007-1 R5. The URE Companies revoke physical and electronic access upon termination of an employee, and changing roles triggers an action to review continued business need and access required. The URE Companies also

implemented automated processes to initiate notifications when an individual's PRA or training is about to expire.

Fourth, the URE Companies provide all assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by the failure to implement password changes and the failure to implement logging and monitoring on some network switches.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plan required the URE Companies to:

1. change all passwords for any device identified as not having met the frequency or complexity requirements;
2. implement interim manual processes to ensure password change frequency and complexity requirements are met;
3. review current ESP electronic access point access request, authorization, and authentication practices against existing formal procedures;
4. revise active directory groups ownership and add new groups to assets where necessary;
5. update existing processes, technical mechanisms, and current procedural documentation;
6. implement tools and technologies for user-level authentication;
7. revise TFEs as necessary;
8. complete a monitoring assessment of generic ID usage procedures;
9. perform a quality assurance review of account logging and monitoring on checkpoint firewalls and network switches;
10. implement a solution to enforce monitoring and logging;
11. identify opportunities and lessons learned to enhance the existing process for reviewing access to user accounts;
12. train relevant personnel; and
13. perform a peer quality assessment of annual user privileges in accordance with designated processes and develop a plan for implementing lessons learned.

CIP-007-1 R6 (RFC2012010084, RFC2012010091, RFC2012010098, NPCC2014013543)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R6. The URE Companies reported that they failed to log properly system events related to cybersecurity for CCAs, other types of protected assets, and access control and monitoring assets.

During the URE2 Compliance Audit, URE2 failed to provide evidence that it performs monitoring of security events as required by its organizational processes and technical and procedural mechanisms. URE2 also failed to provide evidence establishing that it issues alerts for detected Cyber Security Incidents.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R6 for failing to ensure that all Cyber Assets within the ESP implement automated tools or organizational process controls to monitor system events that are related to cybersecurity.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to log system events related to cybersecurity increased the possibility that undetected misuse or compromise of CCAs and other system events that are related to cybersecurity could occur without the URE Companies' knowledge.

However, several factors mitigated the risk. First, although IT vendor personnel were permitted to use a generic user identification, the personnel were required to first authenticate to the corporate environment before accessing electronic access points to the ESP. The URE Companies monitored the vendors' work as it occurred, and all personnel assigned to the generic identification had completed PRAs and CIP training. In addition, the lack of automated monitoring was mitigated by the URE Companies' use of manual logging and reviewing.

Additionally, the URE Companies provide all Cyber Assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by these violations.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. update existing processes, technical mechanisms, and current procedural documentation;
2. document acceptable compensating measures for generic identifications and logging reviews;
3. implement acceptable tools and technologies for user-level authentication;
4. implement process improvements to prevent future gaps with respect to logging;
5. perform a quality assurance review of account logging and monitoring on checkpoint firewalls and network switches; and
6. implement solution to enforce monitoring and logging.

CIP-007-1 R7 (RFC2012010921, RFC2012010925, RFC2013011968, NPCC2014013542)

During the URE2 Compliance Audit, URE2 failed to present evidence demonstrating that it established formal methods, processes, and procedures for the disposal or redeployment of Cyber Assets with the ESP.

Subsequently, URE1 submitted a Self-Report to ReliabilityFirst stating that it did not have sufficient evidence to demonstrate that it established formal methods, processes, and procedures for the disposal or redeployment of Cyber Assets with the ESP. During the URE1 Compliance Audit, ReliabilityFirst confirmed that these facts and circumstances constituted a violation of CIP-007-1 R7.

URE3 later submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit and the URE1 Compliance Audit, it did not have sufficient evidence to demonstrate that it established formal methods, processes, and procedures for the disposal or redeployment of Cyber Assets with the ESP.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R7 for failing to establish formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the ESP.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the violation increased the possibility that non-trained, unauthorized individuals could retrieve sensitive data from the devices.

However, the URE Companies had some protections in place to limit the potential for unauthorized retrieval of data from their Cyber Assets. First, the URE Companies stored any equipment that they removed from service in existing PSPs to limit the risk that sensitive information would be accessible to unauthorized individuals. Second, while their documentation was lacking, the URE Companies sanitized, erased, and destroyed hard drives in all equipment redeployed or removed from service.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. develop a unified policy and procedure to govern the disposal and redeployment of all Cyber Assets;
2. conduct a pilot of the disposal and redeployment procedure;
3. assess the procedure for additional improvements;
4. implement lessons learned into the disposal and redeployment procedure; and
5. develop and deliver training on the procedure.

CIP-007-1 R8 (RFC2012010085, RFC2012010092, RFC2012010099, NPCC2014013540)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R8. The URE Companies reported that they had incomplete lists of ports and services, which did not allow the URE Companies to verify that only ports and services required for operations of the Cyber Assets within the ESPs are enabled. Additionally, during the performance of the CVAs, the URE Companies did not retain documentation to establish compliance with the remaining sub-requirements of CIP-007-1 R8.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R8 for failing to perform an annual CVA of all Cyber Assets within the ESP that included all of the sub-requirements of CIP-007-1 R8.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to perform an

adequate CVA of all Cyber Assets within the ESP at least annually increased the possibility that the URE Companies' systems would be open to cyber vulnerabilities.

However, the URE Companies provided some protections to their systems to reduce the risk of vulnerabilities. Although the URE Companies did not document the implementation of CVA requirements as defined in the Standard, they were conducting vulnerability scanning through a software program. Further, the URE Companies implemented periodic vulnerability scans to identify open ports and services and then evaluated and managed any unusual issues through the scanning process.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. review prior baselining;
2. develop a new process for the baselining of port and services;
3. conduct a baselining of ports and services for each Cyber Asset;
4. revise their documented CVA processes; and
5. implement the annual CVA using the revised processes.

CIP-007-1 R9 (RFC2012010313, RFC2012010301, NPCC2014013539, RFC2012010317)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R9 for failing to review, update, and maintain all documentation to support compliance with the requirements of CIP-007 at least annually. During the URE2 Compliance Audit, ReliabilityFirst confirmed that URE2 did not maintain documentation to demonstrate a review and update of the documentation specified in CIP-007 and confirmed that these facts and circumstances constituted a violation of the Standard.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R9 for failing to annually review and update the documentation specified in CIP-007.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The violations were documentation deficiencies. The URE Companies had documented processes requiring the annual review and approval of CIP-related documentation. The URE Companies were not maintaining sufficient documentation of their annual reviews because their workflow processes did not provide sufficient evidence of compliance (i.e., the dates on which information was approved).

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. review and revise existing annual review processes;
2. develop systematic mechanisms to ensure that an annual review is scheduled for each year;
3. develop an inventory of all CIP-007 documentation subject to review under the revised processes;
4. plan, schedule, and perform an annual review of in-scope documentation; and
5. perform a quality assessment to ensure that all necessary documentation was included in their review processes.

CIP-008-1 R1 (RFC2012010907, RFC2012010926, RFC2013011970, NPCC2014013538)

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to develop and maintain within its Cyber Security Incident response plan a process for ensuring that the plan is reviewed at least annually. Specifically, URE2 developed a stand-alone process for ensuring that the plan is reviewed at least annually, but failed to include this process within the plan itself. URE2 also failed to provide sufficient evidence to demonstrate that it performed annual reviews of the plan.

URE1 submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit, it was also in violation of CIP-008-1 R1 for failing to maintain sufficient evidence to demonstrate that it had completed an annual review of its plan in two prior years. During the URE1 Compliance Audit, ReliabilityFirst also determined that URE1 could not demonstrate that it performed an annual review of the plan for a third year.

URE3 submitted a Self-Report to ReliabilityFirst stating that, based on the URE2 Compliance Audit and URE1 Compliance Audit, it was also in violation of CIP-008-1 R1. Specifically, URE3 could not establish that it conducted an annual review of its plan in two prior years.

ReliabilityFirst determined that the URE Companies had violations of CIP-008-1 R1 for failing to ensure that their Cyber Security Incident response plans are reviewed at least annually. ReliabilityFirst also determined that URE2 failed to develop and maintain within its Cyber Security Incident response plan a process for ensuring that the plan is reviewed at least annually.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The URE Companies maintained a stand-alone process for annual review. URE2's failure to incorporate the stand-alone process for annual review within its Cyber Security Incident response plan was a documentation deficiency. Although their documentation was insufficient, the URE Companies reviewed their Cyber Security Incident response plans annually and in accordance with the standalone process. In addition, no Cyber Security Incidents occurred during the period of the violations.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. develop standardized processes and mechanisms for annually reviewing their Cyber Security Incident response plans;
2. incorporate the standardized processes and mechanisms for annual review into the Cyber Security Incident response plans;
3. conduct an annual review and quality assessment of CIP-008 documentation in accordance with the revised processes; and
4. implement a separate formal review of all CIP documentation to provide additional protection against missed reviews.

The URE Companies each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-009-1 R1 (RFC2012010908, RFC2012010927, RFC2013011971, NPCC2014013547)

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to create and annually review recovery plans for all CCAs. Specifically, although URE2 provided parts of a recovery plan for various types of CCAs, URE2 did not supply a recovery plan that satisfied all of the requirements of a recovery plan as specified by CIP-009-1 R1. ReliabilityFirst also discovered that URE2 failed to specify, within its recovery plan a certain system, the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan, as required by CIP-009-1 R1.1.

URE1 submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit, it also had a violation of CIP-009-1 R1. URE1 reported that it did not have sufficient evidence to demonstrate that it created and annually reviewed recovery plans for all CCAs. During the URE1 Compliance Audit, ReliabilityFirst confirmed that these facts and circumstances constituted a violation of CIP-009-1 R1.

URE3 submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit and the URE1 Compliance Audit, it also had a violation of CIP-009-1 R1. URE3 reported that it did not have sufficient evidence to demonstrate that it created and annually reviewed recovery plans for all CCAs.

ReliabilityFirst determined that the URE Companies had violations of CIP-009-1 R1 for failing to create and annually review recovery plans for all CCAs. In addition, URE2 failed to specify within its recovery plan for a certain system the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through completion of the Mitigation Plans.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failures to create complete recovery plans and review them on an annual basis increased the possibility that the recovery of a failed or compromised CCA could be delayed.

However, the URE Companies did implement mechanisms to protect CCAs against system events. Although the URE Companies did not create recovery plans for all Cyber Asset types, they did implement processes to provide for backup operational capabilities to an alternative site if an entire location was lost and performed periodic failover tests to ensure that operations could in fact be

switched to the alternative site. Additionally, the URE Companies implemented mechanisms to repair or replace individual asset types and to protect CCAs against system events.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. develop consolidated governing documents implementing the CIP-009 recovery plan requirements at the asset type level;
2. develop templates for documenting individual asset type recovery plans;
3. develop updated recovery plans for CIP-009 in-scope assets at the asset type level in accordance with the revised governing documentation and guidance template; and
4. develop and implement training for individuals responsible for activation and implementation of the revised recovery plans.

The URE Companies each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of six hundred and twenty-five thousand dollars ($625,000) for the referenced violations. In addition, ReliabilityFirst will randomly select and perform a Spot Check on one of the three URE Companies in the future.[6] In reaching this determination, ReliabilityFirst considered the following factors:

1. ReliabilityFirst considered one aspect of the URE Companies' compliance history as an aggravating factor in the penalty determination;
2. The URE Companies agreed to undertake a number of above-and-beyond mitigating activities (described more fully below), which ReliabilityFirst considered a mitigating factor in the penalty determination;
3. The URE Companies had an internal compliance program at the time of the violations, aspects of which ReliabilityFirst considered a mitigating factor; however, after determining the full

[6] This Spot Check will be performed with 60 days advance notice and will include: (i) an evaluation of the evidence related to the URE Companies' completion of the above-and-beyond activities described in this Notice of Penalty and the Settlement Agreement; and (ii) a review of the current state of compliance for a random sample of CIP Reliability Standard requirements.

scope of the violations and the mitigation activities, ReliabilityFirst observed that the state of the URE Companies' mitigation activities and compliance had not progressed as quickly as expected considering the number of years they had been working to resolve these violations;

4. The URE Companies self-reported a number of violations, for which ReliabilityFirst awarded partial mitigating credit;
5. The URE Companies were cooperative throughout the compliance enforcement process, for which ReliabilityFirst awarded partial mitigating credit;[7]
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violations individually posed a minimal or moderate risk, and collectively posed a moderate risk, but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

As noted above, the URE Companies have agreed to undertake a series of above-and-beyond mitigating activities which address the management practices that ReliabilityFirst found to be deficient and the root cause of the violations. These above-and-beyond mitigating activities are:

1. implement an annual URE Company-wide forum to address CIP compliance management model documents, present and emerging risks, and mitigating violations;
2. formation of a single office to oversee and monitor all CIP activities across the URE Companies, at a budgeted annual cost;
3. creation of dedicated positions to increase the URE Companies' ability to identify and respond to emerging risks, plan for future activities, and improve decision results, at an annual budgeted cost; and
4. implementation of technological improvements related to CIP compliance and cybersecurity, including for logging, monitoring, and alerting of CIP assets, for configuration management

[7] ReliabilityFirst considered the URE Companies' cooperation with ReliabilityFirst, as well as the collaborative and open nature of their subject matter experts, to be a mitigating factor in the penalty determination. However, ReliabilityFirst reduced this mitigating credit in light of the extended period of time it took for the URE Companies to mitigate and resolve these violations. In particular, ReliabilityFirst considered that the URE Companies routinely requested extensions of mitigation deadlines, often on or near the various due dates for mitigation milestone deliverables.

purposes, and to isolate sensitive segments from the internet and other weaknesses, at a budgeted cost above-and-beyond the costs required for baseline compliance activities.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of six-hundred and twenty-five thousand dollars ($625,000) and the non-monetary penalty of conducting a Spot Check 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[8]

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,[9] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on August 12, 2014 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC also considered the factors considered by ReliabilityFirst, as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of six hundred and twenty-five thousand dollars ($625,000) and the non-monetary penalty of conducting a Spot Check 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.

[8] *See* 18 C.F.R. § 39.7(d)(4).
[9] *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).

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

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

Gerald W. Cauley 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 Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Dr. Cleveland, Ohio 44131 (216) 503-0682 (216) 503-9207 – facsimile bob.wargo@rfirst.org	Sonia C. Mendonça* Associate General Counsel and Senior Director 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

Niki Schaefer* Managing Enforcement Attorney ReliabilityFirst Corporation 3 Summit Park Dr. Cleveland, Ohio 44131 (216) 503-0689 (216) 503-9207 – facsimile niki.schaefer@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Theresa White* Associate Counsel ReliabilityFirst Corporation 3 Summit Park Dr. Cleveland, OH 44131 (216) 503-0667 (216) 503-9207 – facsimile theresa.white@rfirst.org Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, Ohio 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,

/s/ Edwin G. Kichline

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

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
Associate General Counsel and Senior
Director 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: The URE Companies
ReliabilityFirst Corporation

Attachments