NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

January 28, 2016

VIA ELECTRONIC FILING

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

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity 1, Unidentified Registered Entity 2, Unidentified Registered Entity 3, and Unidentified Registered Entity 4, FERC Docket No. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), Unidentified Registered Entity 2 (URE2), Unidentified Registered Entity 3, and Unidentified Registered Entity 4 (Collectively the URE Entities), with information and details regarding the nature and resolution of the violations,[2] 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)).[3]

NERC is filing this Notice of Penalty with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE Entities have entered into a Settlement Agreement to resolve all outstanding

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2015). *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] 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.

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

issues arising from ReliabilityFirst's determination and findings of violations of the CIP Reliability Standards.

According to the Settlement Agreement, URE Entities neither admit nor deny the violations, and have agreed to the assessed penalty of one hundred and fifty thousand dollars ($150,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Accordingly, NERC is filing this Full Notice of Penalty in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between ReliabilityFirst and URE Entities. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

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

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
URE1 RFC2014013798	CIP-002-3	R3	High/ Severe	SC	$150,000
URE1 RFC2014013829	CIP-003-3	R1	Medium/ Severe	SR	
URE1 RFC2014013830	CIP-003-3	R4	Medium/ Severe	SR	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
URE1 RFC2014013799	CIP-003-3	R5	Lower/ Severe	SC	
URE1 RFC2014013800	CIP-003-3	R6	Lower/ Severe	SC	
URE1 RFC2014013831	CIP-004-3	R1	Lower/ Severe	SR	
URE1 RFC2014013832	CIP-004-3	R2	Lower/ Severe	SR	
URE2 RFC2014013446	CIP-004-3a	R2.1	Medium/ Severe	SR	
URE1 RFC2014013801	CIP-004-3	R4	Lower/ Severe	SC	
URE2 RFC2014013794	CIP-004-3a	R4.1	Lower/ Severe	SC	
URE1 RFC2014013802	CIP-005-3a	R1	Medium/ Severe	SC	$150,000
URE1 RFC2014013803	CIP-005-3a	R2	Medium/ Severe	SC	
URE1 RFC2014013804	CIP-005-3a	R3	Medium/ Severe	SC	
URE1 RFC2014013805	CIP-005-3a	R4	Medium/ Severe	SC	
URE1 RFC2014013833	CIP-005-3a	R5	Lower/ Severe	SR	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
URE1 RFC2014013810	CIP-006-3c	R1	Medium/ Severe	SC	
URE2 RFC2015014715	CIP-006-3c	R1	Medium/ Severe	SR	
URE1 RFC2014013811	CIP-006-3c	R2	Medium/ Severe	SC	
URE1 RFC2014013812	CIP-006-3c	R3	Medium/ Severe	SC	
URE4 RFC2014013809	CIP-006-3c	R3	Medium/ Severe	SC	
URE1 RFC2014013813	CIP-006-3c	R4	Medium/ Severe	SC	
URE1 RFC2014013814	CIP-006-3c	R5	Medium/ Severe	SC	
URE1 RFC2014013815	CIP-006-3c	R6	Lower/ Severe	SC	$150,000
URE1 RFC2014013834	CIP-006-3c	R7	Lower/ Severe	SR	
URE1 RFC2014013835	CIP-006-3c	R8	Medium/ Severe	SR	
URE1 RFC2014013820	CIP-007-3a	R1	Medium/ Severe	SC	
URE1 RFC2014013821	CIP-007-3a	R2	Medium/ Severe	SC	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
URE1 RFC2015015243	CIP-007-3a	R3	Lower/ Severe	SR	
URE2 RFC2014013795	CIP-007-3a	R3	Lower/ Severe	SC	
URE1 RFC2014013822	CIP-007-3a	R4	Medium/ Severe	SC	
URE1 RFC2014013823	CIP-007-3a	R5	Lower/ Severe	SC	
URE2 RFC2014014469	CIP-007-3a	R5.2.3	Lower/ Severe	CA	
URE3 RFC2014013797	CIP-007-3a	R5	Lower/ Severe	SC	
URE4 RFC2014013816	CIP-007-3a	R5	Lower/ Severe	SC	
URE1 RFC2014013824	CIP-007-3a	R6	Lower/ Severe	SC	$150,000
URE1 RFC2014013915	CIP-007-3a	R7	Lower/ Severe	SR	
URE1 RFC2014013825	CIP-007-3a	R8	Lower/ Severe	SC	
URE1 RFC2014013836	CIP-007-3a	R9	Lower/ Severe	SR	
URE1 RFC2014013826	CIP-008-3	R1	Lower/ Severe	SC	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
URE1 RFC2014013827	CIP-009-3	R1	Medium/ Severe	SC	

Background

ReliabilityFirst resolved all of these violations together because the URE Entities all share a common parent company and now implement the parent company's unified CIP compliance program.

Prior, the current parent company acquired URE1 from its original parent company and acquired another subsidiary company that controlled some of the operations of the original parent company. After a number of events, the original parent company filed for Chapter 11 bankruptcy. The bankruptcy filing caused uncertainty regarding the future of the original parent company and its subsidiary company, thus resulting in voluntary departures from both organizations. The loss of resources and leadership in personnel actively engaged in the CIP compliance program created a foundation for the violations.

Before the acquisition of URE1, the current parent company merged with the former parent company of URE2, URE3, and URE4. Although URE2, URE3, and URE4 continue to operate under the former parent company umbrella, the current parent company became the legal owner of that umbrella company and is now the ultimate parent company for the three URE Entities included in this Settlement Agreement.

After these acquisitions, the current parent company updated its CIP compliance program so that the parent and its subsidiaries have one unified CIP compliance program.

RFC2014013798 CIP-002-3 R3- OVERVIEW

ReliabilityFirst determined that the former subsidiary company violated CIP-002-3 R3 by failing to identify, as part of its Critical Cyber Asset identification process, multiple devices as Critical Cyber Assets (CCAs) that were essential to the operation of its Critical Assets. Specifically, the former subsidiary company failed to appropriately classify as CCAs several devices that used a routable protocol to communicate outside of the Electronic Security Perimeter (ESP) or used a routable protocol to communicate within a control center.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). First, an accurate list of CCAs is fundamental to ensuring that all CCAs are afforded the protections required by the CIP Reliability Standards. Therefore, former subsidiary's failure to maintain an accurate list of CCAs increases the likelihood of further violations of other CIP Reliability Standards. Second, the duration of the violation indicates that the subsidiary failed to identify and correct the issue in a timely manner, which also increased the likelihood of further violations of other CIP Reliability Standards. The risk posed by the foregoing facts and circumstances was mitigated by the fact that the subsidiary had several measures in place to protect and restrict access to the mistakenly excluded CCAs both logically and physically. Logically, these devices were protected by being on a restricted network, having password protections on the connections to the network systems, and several other protective measures including intrusion detection, logging, and anti-malware programs. Physically, access to these devices was also highly restricted to authorized personnel with multiple physical access control layers within a non-public, controlled space. These devices were in a secured facility and under constant surveillance.

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

URE1 submitted its Mitigation Plan designated RFCMIT011314 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. use the current parent company's CCA identification program to ensure that processes are in place to include consideration and identification of all Cyber Assets;
2. identify all applicable Cyber Assets;
3. implement the current parent company's CCA Identification Program to ensure that all CCAs are identified and documented; and
4. provide training for all appropriate personnel regarding CCA identification.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013829 CIP-003-3 R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary company violated CIP-003-3 R1 by failing to document and implement a cyber security policy that addressed all of the aspects required by CIP-003-3 R1. Specifically, the deficient cyber security policy: a) did not adequately address the requirements of CIP-002-3 through CIP-009-3; and b) was annually reviewed, but was not reviewed and approved by the senior manager assigned pursuant to R2.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk posed by the foregoing facts and circumstances was mitigated by the fact that the subsidiary did have a documented and implemented cyber security policy that represented management's commitment and ability to secure its CCAs. This policy was annually reviewed by the subsidiary's management, but not by the senior manager identified in CIP-003-3 R2.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when the subsidiary formally adopted and implemented an adequate cyber security policy.

URE1 submitted its Mitigation Plan designated RFCMIT011234 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. modify the cyber security policy and the security management controls program documentation to include the necessary elements for compliance with CIP-003-3; and
2. approve the cyber security policy and the security management controls program.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013830 CIP-003-3 R4- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-003-3 R4 by failing to implement and document a program to identify, classify, and protect information associated with CCAs as required by CIP-003-3 R4. Furthermore, even after formalizing the security management controls program, the subsidiary had not yet annually assessed adherence to its CCA information protection program, including documentation of the assessment results as required by CIP-003-3 R4.3.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The lack of a formal, documented security management controls program prevents an entity from ensuring that responsible personnel are performing the necessary activities to protect CCA information. An undocumented program increases the likelihood of human error, which may result in protected CCA information being compromised. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. First, the generation assets potentially affected by this violation have not been determined to be critical. Second, the logical and physical access controls in place with respect to CCAs also operate to protect CCA information.

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

URE1 submitted its Mitigation Plan designated RFCMIT011225 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation of the security management controls program that identifies, classifies, and protects information associated with CCAs as required by CIP-003-3 R4 and 4.1;
2. develop and document an assessment methodology to assess the adherence to the CCA information protection program;
3. assess the adherence to the CCA information protection program, including documentation of the assessment results as required by CIP-003-3 R4.3;
4. implement an action plan to remediate deficiencies identified during the assessment; and
5. train individuals responsible for the protection of CCA information and assessment of the program to ensure ongoing compliance.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013799 CIP-003-3 R5- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-003-3 R5 by failing to: a) have a documented program for managing access to protected CCA information; b) annually verify the list of personnel responsible for authorizing access privileges to protected information to confirm that access privileges were correct and that they corresponded with the subsidiary's needs and appropriate personnel roles and responsibilities; and c) assess and document the processes for controlling access privileges to protected information.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The access controls called for by CIP-003-3 R5, specifically maintaining an access list and performing periodic verification of logical and physical access to protected information, are an integral part of an entity's CIP compliance program. Thus, inadequate access controls may allow for unauthorized access to such information and may result in violations of several other CIP Reliability Standards and Requirements. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. First, the logical and physical access controls in place with respect to CCAs also operate to protect CCA information. Second, the subsidiary stored relevant information

on restricted networks and limited access to those individuals with a business need to access the information.

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

URE1 submitted its Mitigation Plan designated RFCMIT011221 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation which details program for managing access to protected CCA information as required by CIP-003-3 R5 and 5.1;
2. verify and create the list of personnel responsible for authorizing access to protection information;
3. have approved individuals review the list of user access privileges and roles and responsibilities to ensure that the list is appropriate;
4. develop and document an assessment methodology to assess the process for controlling access privileges to protected information;
5. assess the process for controlling access privileges to protected information, including documentation of the assessment results; and
6. train individuals, who are responsible for the program for managing access to protected CCA information, on the process to ensure ongoing compliance.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013800 CIP-003-3 R6- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-003-3 R6 by failing to have a formally documented change control or configuration management process for the activities required in R6. Rather, the subsidiary only had an informal change management process including a ticketing system to approve and track master change requests for all changes to CCAs as well as other Information Technology (IT) assets.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of a formal change control and configuration management process can result in serious vulnerabilities and increased threat levels. Without such a process, an entity may be unable to identify unauthorized changes to its system or to determine the extent of a possible intrusion. The

risk posed by the foregoing facts and circumstances was mitigated by subsidiary's informal change management process that was in place during the period of noncompliance. As stated above, this informal process included a ticketing system to approve and track master change requests for all changes to CCAs as well as other IT assets.

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

URE1 submitted its Mitigation Plan designated RFCMIT011215 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop a formal, documented change management processes for compliance with CIP-003-3; and
2. approve the documented change management processes to ensure ongoing security.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013831 CIP-004-3 R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-004-3 R1 by failing to document its security awareness program to ensure that personnel with authorized cyber or unescorted physical access to CCAs received ongoing awareness reinforcement in sound security practices. Rather, the subsidiary only had an informal, undocumented communication plan in place for security awareness for such personnel.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The lack of a formal security awareness program increases the likelihood that responsible personnel may not be aware of the latest security threats. Cyber threats, in particular, are constantly evolving, which requires responsible personnel to keep updated on an ongoing basis. The risk posed by the foregoing facts and circumstances was mitigated by the informal communication plan that the subsidiary had in place. Pursuant to this plan, responsible personnel would keep each other updated on any new threats or security issues of which they became aware.

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

URE1 submitted its Mitigation Plan designated RFCMIT011216 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation of the cyber security awareness and training program for CIP-004-3a; and
2. approve that documentation.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013832 CIP-004-3 R2- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-004-3 R2 by failing to have a documented cyber security training program for personnel having authorized cyber or authorized unescorted physical access to CCAs. Moreover, once the subsidiary implemented a program, the training did not specifically address the minimum topics included in the sub-requirements of CIP-004-3 R2. Specifically, the program did not cover action plans and procedures to recover or re-establish CCAs and access thereto following a cyber security incident. Additionally, while this recovery training was provided as ancillary training, not all relevant personnel were involved.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of a formal cyber security training program increases the likelihood that untrained personnel may have cyber or unescorted physical access to CCAs. In this case, at least some of the subsidiary's personnel, who were responsible for recovery following a cyber security incident, were not involved in any training related to recovery testing.

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

URE1 submitted its Mitigation Plan designated RFCMIT011226 to address the referenced violations. URE1's Mitigation Plan required URE1 to develop a formal, documented annual cyber security training program, and train all responsible individuals on the annual cyber security training program to ensure ongoing security.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013446 CIP-004-3a R2.1- OVERVIEW

ReliabilityFirst determined that on two separate occasions, both of which occurred prior to URE2's transitioning to the current parent company's CIP compliance program, URE2 granted certain individuals, who had not completed the requisite training, access to a Physical Security Perimeter

(PSP). A security officer, who was newly hired by a contracted security service, erroneously escorted a cleaning crew into a designated PSP without proper authorization and documentation. The cleaning crew remained within the PSP for a total of 25 minutes. On a different occasion, an individual was granted access to a PSP without proper training during the commissioning of a new PSP area. Although URE2 had completed a Personnel Risk Assessment (PRA) for this individual, he had not completed the required training prior to obtaining access. URE2 removed his access on a later date that year.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. In the first instance, the cleaning crew was escorted into the PSP by an individual with authorized unescorted physical access. The cleaning crew was in the PSP for only a short period of time during which CIP-trained and authorized personnel were present and observed the cleaning crew's actions. In the second instance, the individual had passed the PRA. ReliabilityFirst also notes that access records indicate that this individual did not access the PSP during the time he had unauthorized access to it.

ReliabilityFirst determined the duration of the violation to be from the date that the cleaning crew was improperly granted access to a PSP in the first instance, through the date on which URE2 removed PSP access for the individual in the second instance.

URE2 submitted its Mitigation Plan designated RFCMIT011423-1 to address the referenced violations. URE2's Mitigation Plan required URE2 to:

1. change the security officers' passwords to prevent sharing;
2. ensure that hard copies of security procedures are readily available at the security desk;
3. assign unique credentials to each security officer to further prevent sharing among security officers;
4. review current practices and guidelines for providing NERC CIP physical access and visitor access, lost or forgotten identifications and/or passwords, and escort requirements; and
5. develop a process of notification when security officers are requested to be added, changed or removed, a change ticket must be completed to ensure that new officers received proper training, background checks, and are receiving the appropriate access or revocation.

RFC2014013801 CIP-004-3 R4- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-004-3 R4 by failing to maintain complete lists of personnel with authorized cyber or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs, missing 15% or more of the

authorized personnel. Furthermore, the subsidiary did not review the list(s) of all personnel who have access to CCAs quarterly, nor did the subsidiary update the list(s) within seven calendar days of any change of personnel with such access to CCAs, nor any change in the access rights of such personnel. The subsidiary also failed to revoke access to CCAs within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer required such access to CCAs.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The failure to maintain a current and accurate list of personnel with cyber or unescorted physical access to CCAs increases the likelihood that a cyber-attacker could obtain unauthorized access to the CCAs. The risk posed by the foregoing facts and circumstances was mitigated by several additional controls that were in place during the period of noncompliance. For instance, access to the CCAs was highly restricted both physically and logically. All currently identified CCAs are in a secured facility with multilayered physical security controls to restrict physical access. The primary assets are located in a secured data center which provides an attestation of the controls environment and the backup generation management system (GMS) is located in a secured room. The CCAs are also continuously monitored and logged, sit behind an ESP with intrusion detection, have antivirus and malware prevention tools installed, and are contained within a restrictive network.

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

URE1 submitted its Mitigation Plan designated RFCMIT011235 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the current parent company's access control program to install the Energy Management System (EMS) integrated system on the affected CCAs to ensure that the proper processes are in place for quarterly review and update of the Master Access List;
2. identify individuals who should be on the Master Access List prior to the EMS migration;
3. review and certifying that each individual to be authorized has completed the appropriate credentials and document the authorization updates within the Master Access List; and
4. train appropriate personnel on the actions necessary for compliance with CIP-004-3 R4.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013794 CIP-004-3a R4.1- OVERVIEW

ReliabilityFirst determined that prior to transitioning to the current parent company's CIP compliance program, URE2 violated CIP-004-3a R4 by: a) failing to update its CCA personnel access list within 7 days of an access change; and b) granting PSP access to an individual who did not receive access approval for that area.

For the first instance, during the integration of URE2, URE3, and URE4 and the current parent company and the corresponding installation of the EMS system, access change requests were submitted via multiple ticketing systems. The parties responsible for maintaining the access documentation were not receiving all of the necessary notifications of access requests. Consequently, those responsible individuals failed to update the access lists within the appropriate time frame. In all cases, the access was approved and proper PRAs were performed.

For the second instance, during the commissioning of a new PSP, an individual was granted access to the new PSP without proper approval. Prior to the declaration of the area as a PSP, but after construction was completed, access was provided to those individuals working in the new room. Due to the number of individuals with access to the area, the normal ticketing process was not used where a ticket for each individual would have been entered. Instead, all parties requiring access were processed as a group with PRA and training being tracked prior to requesting approval for access. Although the individual was on the original group tracking list, he was not on the list submitted for approval. On the date the individual needed access, the individual required access to the area for the first time. The access provider, seeing his name on the original tracking list, assumed he was approved for access and provided an access card. Since the individual was not included in the original group approval, he did not have proper approval for access.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. First, although access changes were not completed within the appropriate timeframe, all access changes were approved and PRAs were completed. In addition, logical access controls were still in place. Specifically, the devices at issue are enclosed within an ESP protected by firewalls and monitored per the CIP-005-3 requirements. Moreover, the devices at issue were located on isolated networks to prevent exposure to untrusted networks. Second, the instances of noncompliance were the result of unique circumstances which occurred during the merger between URE2 and the current parent company, but prior to URE2's transitioning to the parent company's CIP compliance program.

ReliabilityFirst determined the duration of the violation to be from when the individual was improperly granted access to the PSP, through when URE2 completed its Mitigation Plan.

URE2 submitted its Mitigation Plan designated RFCMIT011397 to address the referenced violations. URE2's Mitigation Plan required URE2 to consolidate access requests into a single system requiring verification of credentials before commissioning.

URE2 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE2 had completed all mitigation activities.

RFC2014013802 CIP-005-3a R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-005-3a R1 by failing to: a) identify and document all access points to the perimeter(s); b) identify and protect one or more noncritical Cyber Assets within a defined ESP to the requirements of Standard CIP-005, c) afford Cyber Assets used in the access control and/or monitoring of the ESP(s) one or more of the required protective measures of R1.5; and d) maintain documentation of some interconnected critical and noncritical Cyber Assets within the ESP(s), electronic access points to the ESP(s), and Cyber Assets deployed for the access control and monitoring of these access points.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The failure to identify and adequately protect the ESP, as well as all access points on the ESP, could have led to serious harm to the BPS by increasing the likelihood that cyber intrusions could have occurred resulting in damage to various critical and noncritical Cyber Assets.

The risk posed by the foregoing facts and circumstances was partially mitigated by the following factors. First, all currently identified CCAs reside within a defined ESP, and the subsidiary had measures in place to protect and restrict access to the ESP and physical access to the devices themselves. Specifically, the subsidiary had electronic logging to monitor access to the ESPs, password protections on the connections to the network systems, and other protective measures including intrusion detection and anti-malware. Furthermore, physical access to the ESP devices was highly restricted to appropriate personnel with multiple physical access control layers within a non-public, controlled space. The ESP devices are in a secured facility, under constant surveillance, and are located in a secured data center, which provides an attestation of the controls environment, and the backup GMS is located in a secured room. All doorways to the secured rooms at each location are alarmed for forced entry and monitored with cameras. Additionally, the electronic access control and monitoring devices were protected by the subsidiary's cyber security policies and procedures, and the people accessing those devices had received cyber security training and have PRAs on file. Finally, although not all assets were listed on the ESP documentation, documentation of the ESP and related assets exists in multiple forms such as a Visio diagram and asset lists.

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

URE1 submitted its Mitigation Plan designated RFCMIT011319 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the current parent company's NERC CIP-005 compliance program and perform a preliminary ESP and electronic access point design to ensure that every CCA resides within an ESP and that the ESP and all access points to it have been properly identified and documented;
2. validate the new configuration to ensure that all CCAs and access points are properly identified and documented; and
3. train all appropriate personnel on the actions necessary for compliance with CIP-005-3a R1.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013803 CIP-005-3a R2- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-005-3a R2 by failing to: a) document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESPs; b) use an access control model with respect to its processes and mechanisms that denies access by default, such that explicit access permissions must be specified; c) ensure that, at one or more access points to the ESPs, only ports and services required for operations and for monitoring Cyber Assets within the ESP were enabled, or document, individually or by specified grouping, the configuration of those ports and services; d) implement strong procedural or technical controls at the access points where external interactive access into the ESP had been enabled, to ensure authenticity of the accessing party, where technically feasible; and e) maintain all appropriate documentation.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The failure to formally implement and document the organizational processes and technical and procedural mechanisms in place to control electronic access to the ESPs could have led to serious harm to the BPS by increasing the likelihood that cyber intrusions could have occurred resulting in damage to various critical and noncritical Cyber Assets. The risk posed by the foregoing facts and circumstances was mitigated by the logical and physical access controls.

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

URE1 submitted its Mitigation Plan designated RFCMIT011316 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the parent company's NERC CIP-005 Compliance Program and associated procedures for URE1's Cyber Assets to perform a preliminary network design of electronic access control and monitoring (EACM) of ESP access points;
2. identify technical and procedural mechanisms for electronic access control and monitoring of ESP access points as part of the electronic access controls program re-design change control process;
3. implement the resulting new configuration to ensure that all technical and procedural EACMs at ESP access points are documented and in place; and
4. train appropriate personnel on the actions necessary for compliance with CIP-005-3a R2.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013804 CIP-005-3a R3- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-005-3a R3 by failing to document electronic or manual processes for monitoring and logging access points to the ESPs twenty-four hours per day, seven days per week. Also, even though technically feasible, the subsidiary failed to implement security monitoring processes to detect and alert for attempted or actual unauthorized accesses. Rather, the subsidiary relied on manual review of generated logs.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of formal, documented electronic or manual processes for monitoring and logging access points to the ESPs poses a serious risk to the reliability of the BES because it increases the likelihood that an individual could obtain unauthorized access to the ESP without leaving any record of the intrusion.

The risk posed by the foregoing facts and circumstances was mitigated by the following factors. Although undocumented, the subsidiary utilized manual processes for monitoring and logging access at access points to the ESPs twenty-four hours per day, seven days per week. Specifically, the subsidiary utilized an intrusion detection program, among other tools, to monitor and log access. The resulting logs of attempted or actual unauthorized accesses were reviewed at least every 90 calendar days.

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

URE1 submitted its Mitigation Plan designated RFCMIT011317 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. as part of the parent company's EMS integrated system change control and commissioning process, identify systems for continuous monitoring and logging of access at ESP access points, as well as protocols for receiving alerts and alarm response;
2. utilize the parent company's NERC CIP-005 compliance program and associated procedures to design technical controls for access monitoring, logging, and alerting at ESP access points;
3. implement and documenting the new configuration to ensure that monitoring and logging of ESP access points is taking place and that alerting and alarm response protocols are enabled; and
4. train appropriate personnel on the actions necessary for compliance with CIP-005-3a R3.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013805 CIP-005-3a R4- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-005-3a R4 by failing to perform a Cyber Vulnerability Assessment (CVA) at least annually for one or more of the access points to the ESPs, and the CVA, once performed, did not include one or more of the sub-requirements of R4. Specifically, some devices were not included in the CVA, and the CVA did not include an action plan to remediate or mitigate vulnerabilities identified during the CVA and the execution status of that plan.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The failure to perform a CVA prevented the subsidiary from identifying inherent vulnerabilities associated with its CCAs. Allowing such vulnerabilities to remain unknown increases the risk that an individual could gain unauthorized access to CCAs within the ESP and cause harm to the integrity of the CCAs. The risk posed by the foregoing facts and circumstances was mitigated by the logical and physical access controls.

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

URE1 submitted its Mitigation Plan designated RFCMIT011312 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. perform a CVA in accordance with the required vulnerability assessment process, review and verify that only ports and services required for operations at these access points are enabled, review controls for default accounts, and document the results of the CVA;
2. develop an action plan for the CVA and document the execution status of that action plan;
3. utilize the parent company's NERC CIP-005 Compliance Program and associated procedures for the EMS integrated system to gather the required information for the CVA;
4. define the scope of work for the CVA that is required; and
5. train appropriate personnel on the actions necessary for compliance with CIP-005-3a R4.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013833 CIP-005-3a R5- OVERVIEW

ReliabilityFirst determined that prior to being acquired by the current parent company, the former subsidiary violated CIP-005-3a R5 by failing to formally define the documentation that would be required for compliance with CIP-005-3. Therefore, the subsidiary failed to review, update, and maintain any such documentation.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The violation is a documentation issue. ReliabilityFirst also notes that the subsidiary identified no known instances where a change to the network or controls was made that would have necessitated a corresponding change in documentation because only minimal system hardware or software changes occurred during the period of this violation.

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

URE1 submitted its Mitigation Plan designated RFCMIT011304 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation of the cyber security ESP Program for CIP-005-3a;

2. implement a process of formal review and attestation of review for the cyber security ESP Program to ensure that documentation is updated to reflect a modification of the network controls within 90 calendar days of the change; and
3. have a committee to create an attestation of review for ongoing process improvement for CIP-005-3a compliance.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013810 CIP-006-3c R1- OVERVIEW

ReliabilityFirst determined that the subsidiary violated CIP-006-3c R1 by failing to ensure that its physical security plan: a) addressed and included processes to ensure and document that all Cyber Assets within an ESP also reside within an identified PSP; b) identified all access points through each PSP; c) included processes, tools, and procedures to monitor physical access to the perimeter(s); d) addressed the appropriate use of physical access controls as described in R4; and e) met the requirements of continuous escorted access of visitors within the PSP. Moreover, the current physical security perimeter plan failed to accurately identify the PSP. The plan identified the PSP inaccurately as the room in which the GMS sits, rather than the more appropriate identification of the PSP as the cabinet in which the currently identified CCAs reside.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. First, although the subsidiary's documentation lacked many elements required by CIP-006-3c R1, it had a physical security plan that addressed the identification of a PSP, protection of Physical Access Control Systems (PACS), protection of electronic access controls systems, physical access controls, monitoring physical access, logging physical access, access log retention, and maintenance and testing related to the PACS identified in the plan. Second, while a true "six-wall border" was not in place, physical access to all currently identified CCAs was highly restricted.

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

URE1 submitted its Mitigation Plan designated RFCMIT011230 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the parent company's NERC CIP-006 Compliance Program to design new PSPs for physical protection of CCAs and associated controls;
2. build new PSPs and implement appropriate controls;

3. revise the parent company's physical security plan documentation to include URE1's physical access controls; and
4. train appropriate personnel the design, implementation, and maintenance of the new physical security plan.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2015014715 CIP-006-3c R1- OVERVIEW

ReliabilityFirst determined that URE2 violated CIP-006-3c R1 by allowing an unauthorized cleaning contractor to access a PSP without an escort at URE2. The first instance of this violation occurred when an authorized contractor swapped his daily cleaning duties with an unauthorized coworker. In doing so, the authorized contractor passed his access badge to the unauthorized cleaning contractor, enabling the contractor to gain access into the side door of the PSP for a total of five hours. The second instance of this violation occurred over the course of six days. In this instance, the same authorized contractor was preparing to leave for vacation and passed his access badge to an unauthorized contractor, enabling that unauthorized individual to gain access to a PSP without an escort for a total of six hours. In both instances, the use of the authorized swapped badge was detected by a shift supervisor or facilities management and the unauthorized personnel were removed from the PSP. Also, in both instances, the authorized contractor who swapped his badge did not understand the restrictions around sharing his badge with unauthorized personnel and the unauthorized contractors did not follow proper protocol for obtaining a continuous escort while accessing the PSP.

Review of the PSP and CCAs indicates that there was no compromise of assets and incident review with the contractors indicates that there was no malicious intent on the part of the authorized contractor, nor the unescorted visitors. In addition, in each of these circumstances, a current parent company authorized party was present within the PSP.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. First, URE2 was aware whenever the cleaning crew was within the PSP. Second, authorized personnel were present within the PSP each time that an unauthorized cleaning contractor was present. ReliabilityFirst also notes that, as stated above, a review of the PSP and CCAs indicates that there was no compromise of assets and incident review with the contractors indicates that there was no malicious intent on the part of the authorized contractor, nor the unescorted visitors.

ReliabilityFirst determined the duration of the violation to be from when the first unauthorized contractor was granted access to the PSP, through the last date on which an unauthorized contractor accessed the PSP.

URE2 submitted its Mitigation Plan designated RFCMIT011508 to address the referenced violations. URE2's Mitigation Plan required URE2 to:

1. conduct an incident review with management for the cleaning contracting company;
2. evaluate alternate cleaning contract company sourcing;
3. make a sourcing contract change;
4. conduct PRAs and training for three new cleaning personnel; and
5. review physical access escorting protocol with new contractor management.

RFC2014013811 CIP-006-3c R2- OVERVIEW

ReliabilityFirst determined that prior to being acquired by the current parent company, the former subsidiary violated CIP-006-3c R2 by failing to afford the protective measures specified in CIP-003-3, CIP-004-3 R3, CIP-005-3 R2 and 3, CIP-006-3 R4 and 5, CIP-007-3, CIP-008-3, and CIP-009-3 for all Cyber Assets that authorize and/or log access to the PSPs, such as electronic lock mechanisms and badge readers.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. First, although the PACS were not afforded all of the required protections, they were protected by a corporate security standard that included limited access, both physically and logically, and utilized antivirus and antimalware tools. Second, the PACS are on isolated networks and are independent of the ESPs containing CCAs. Therefore, unauthorized electronic access to PACS devices would not, in itself, lead to the compromise of CCAs or other Cyber Assets within the ESP.

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

URE1 submitted its Mitigation Plan designated RFCMIT011223 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. design and identifying new PACS to be used for change control and configuration planning;
2. implement the new PACS and ensure appropriate controls are applied;
3. revise the parent company's PSP program documents to include URE1's PACS; and

4. train appropriate personnel on the actions necessary for compliance with CIP-006-3c R2.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013812 CIP-006-3c R3- OVERVIEW

ReliabilityFirst determined that URE1 violated CIP-006-3c R3 by failing to properly identify a formal PSP within which Cyber Assets used in the access control and/or monitoring of the ESPs reside. URE1 incorrectly identified its PSP, thus resulting in the corresponding violation of CIP-006-3c R3.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Although URE1 did not have a properly identified PSP, the physical security mechanisms were in place and applied to the Cyber Assets responsible for the access control and/or monitoring of the ESPs. Thus, the likelihood that an individual could have gained unauthorized physical access to the Cyber Assets within the PSP was low.

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

URE1 submitted its Mitigation Plan designated RFCMIT011231 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. ensure that newly identified EACMS will be protected within a PSP as part of the PSP re-designs for change control planning;
2. implement new EACMS and ensure appropriate PSP and PACS controls are applied;
3. revise the parent company's PSP documents to include URE1's EACMS; and
4. train appropriate personnel on the actions necessary for compliance with CIP-006-3c R3.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013809 CIP-006-3c R3- OVERVIEW

ReliabilityFirst determined that URE4 violated CIP-006-3c R3 by permitting a Cyber Asset used in the access control and/or monitoring of the ESP to reside outside of an identified PSP. Specifically, URE4 had a firewall contained within a communications room, but not within a declared PSP.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the firewall was afforded protection under CIP-005 R1.5 except being protected within a PSP. Second, the area where the firewall resides is located in an interior part of the administration building which is key-locked and not available to the general public. Third, the firewall was further protected by restricted access to each overall facility including, but not limited to, guard service, perimeter fencing, and operator rounds checking for intrusion. ReliabilityFirst also notes that logs for the system monitoring this device did not show evidence of ESP activity resulting from physical intrusions during the period of this violation.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE4 completed its Mitigation Plan.

URE4 submitted its Mitigation Plan designated RFCMIT011438-1 to address the referenced violations. URE4's Mitigation Plan required URE4 to:

1. implement and commission a new PACS;
2. reconfigure its Cyber Assets so that they are protected within a PSP; and
3. update the PSP documentation to reflect the new configuration.

RFC2014013813 CIP-006-3c R4- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-006-3c R4 by failing to document the operational and procedural controls to manage physical access at all access points to the PSP(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: card key, special locks, security personnel, or other authentication devices such as biometric, keypad, token, or other equivalent devices that control physical access to the CCAs.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although the requisite operational and procedural controls were not properly documented, URE1 had many of them in place including the use of card keys, man trap systems, cyber locks, security personnel responsible for controlling physical access, biometric readers, and keypads. Accordingly, URE1 had multiple physical access control layers within a nonpublic, controlled space which was under constant surveillance.

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

URE1 submitted its Mitigation Plan designated RFCMIT011232 to address the referenced violations. URE1's Mitigation Plan required URE1 to develop formal documentation of the physical security plan which contains the operation and procedural controls to manage physical access at all access points to the PSP as required by CIP-006-3c.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013814 CIP-006-3c R5- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-006-3c R5 by failing to document or implement the technical and procedural controls for monitoring physical access at all access points to the PSP(s) twenty-four hours a day, seven days a week using one or more of alarm systems or human observation of access points. Specifically, alarm systems or human observation specific to the restricted access cabinet (representing the PSPs) were not addressed.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Although alarming or human observation was not in place specifically related to the cabinets containing the CCAs, these (and the other physical access tools) were in place to restrict physical access. These additional protections reduced the likelihood that an individual could have gained unauthorized access to the PSP

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

URE1 submitted its Mitigation Plan designated RFCMIT011233 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. as part of the PSP re-design, ensure that all PSP physical access points will have appropriate technical and procedural controls for access monitoring twenty-four hours per day, seven days per week;
2. implement new PACS equipment and processes for monitoring PSP physical access points;
3. revise the current parent company's physical security plan documents to include URE1's physical access controls monitoring; and
4. train appropriate personnel on the actions necessary for compliance with CIP-006-3c R5.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013815 CIP-006-3c R6- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-006-3c R6 by failing to implement or document the technical and procedural mechanisms for logging physical entry at all access points to the PSP(s) using one or more of the following logging methods or their equivalent: computerized logging, video recording, or manual logging. Specifically, logging of the physical access to the cabinet representing the PSPs was not addressed.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although they were undocumented, URE1 had several technical and procedural mechanisms in place for logging physical entry at all access points to the PSPs including the use of cyber lock access logs, card reader access logs, manual logs, biometric and keypad logs, and a video log of access. Accordingly, URE1 had multiple physical access logging layers of access to a restricted non-public, controlled space containing the locked cabinets and logs related to the access of the cabinets themselves.

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

URE1 submitted its Mitigation Plan designated RFCMIT011219 to address the referenced violations. URE1's Mitigation Plan required URE1 to develop a formal physical security plan process to include documentation of the technical and procedural mechanisms for logging physical entry at all access points to the PSPs in compliance with CIP-006-3c.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013834 CIP-006-3c R7- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-006-3c R7 by failing to retain physical access logs for at least ninety days. Specifically, the subsidiary failed to retain logs for physical access to the locked cabinets containing CCAs.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although logs were not retained for ninety days for the locked cabinet representing the PSP, the subsidiary had other mechanisms in place for logging physical entry at all access points to the PSPs include the use of card reader logs, manual logs, biometric scan and keypad logs, and video log of access. Logs generated via these mechanisms were retained for 90 days as a matter of policy.

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

URE1 submitted its Mitigation Plan designated RFCMIT011220 to address the referenced violations. URE1's Mitigation Plan required URE1 to implement the cyber lock system, which provided the ability to log physical access to the locked cabinets, and to maintain those logs for 90 calendar days.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013835 CIP-006-3c R8- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-006-3c R8 by failing to have a formal, documented physical security plan that contained a maintenance and testing program.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The former subsidiary implemented a maintenance and testing program within the three-year cycle called for in CIP-006-3c R8. However, that program was not fully adequate because it did not address all of the components required by CIP-006-3c R8. Nevertheless, the tests verified that the risk was minimal, as several physical security mechanisms were in place prior the documentation of the testing program, which secured the PSP.

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

URE1 submitted its Mitigation Plan designated RFCMIT011224 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. as part of the PSP re-design, ensure that all new PACS and physical security systems will have appropriate maintenance and testing programs;
2. ensure that its physical security plan includes testing and maintenance schedules for associated physical security system and physical access controls to ensure proper functioning;
3. ensure that the current parent company's physical maintenance and testing program includes updated documentation for the new URE1's PSP, retention of access controls outage records, logging and monitoring; and
4. train appropriate personnel on the actions necessary for compliance with CIP-006-3c R8.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013820 CIP-007-3a R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R1 by failing to document the cyber security test procedures necessary to minimize the effects of changes to the production environment. Moreover, the subsidiary failed to: a) perform testing for all changes that met the definition of "significant" contained in CIP-007-3a R1; and b) document that testing was done in a manner that reflects the production environment. Finally, the subsidiary retained documentation for some changes, but inaccurately determined that testing was not necessary.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of documented cyber security test procedures increases the likelihood that the subsidiary could introduce new Cyber Assets to the ESP or make significant changes to existing Cyber Assets within the ESP without knowledge of potential adverse effects to the subsidiary's cyber security controls changes. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. The subsidiary had an informal change management process in place that utilized a ticketing system to approve and track master change requests for all changes to currently identified CCAs. This process included the documentation of testing, when the subsidiary deemed testing to be appropriate.

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

URE1 submitted its Mitigation Plan designated RFCMIT011311 to address the referenced violations. URE1's Mitigation Plan required URE1 to develop a formal, documented cyber security testing program necessary to minimize the effects of changes to the production environment, and to train all responsible individuals on the cyber security testing program and revised procedures to ensure ongoing security.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013821 CIP-007-3a R2- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R2 by failing to establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled. Also, the subsidiary: a) enabled one or more ports or services not required for

normal and emergency operations on Cyber Assets inside the ESP; b) did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the ESP; and c) for cases where unused ports and services cannot be disabled due to technical limitations, did not document compensating measure(s) applied to mitigate risk.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. This failure increased the likelihood of infiltration of unauthorized network traffic into the ESP through ports and services that are not necessary for normal or emergency operations, but nevertheless remain enabled. This type of infiltration could cause significant harm to URE1's CCAs. The risk posed by the foregoing facts and circumstances was mitigated by the logical and physical access controls

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

URE1 submitted its Mitigation Plan designated RFCMIT011310 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the current parent company's NERC CIP-007 compliance program and associated procedures of URE1's Cyber Assets, ensuring that (change control) commissioning design of ports and services configuration includes processes to: a) baseline ports and services; b) disable unneeded ports and services; and c) properly justify all enabled ports and services;
2. initially document baseline ports and service targets and justifications;
3. implement baseline process to align URE1's ports and services with compliance program documentation; and
4. train appropriate personnel on the actions necessary for compliance with CIP-007-3a R2.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2015015243 CIP-007-3a R3- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R3 by: a) failing to implement or document, either separately or as a component of the documented configuration management process specified in CIP-003-3 R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP(s); b) failing to document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades;

c) failing to document the implementation of applicable security patches as required in R3 or where an applicable patch was not installed; and d) failing to document the compensating measure(s) applied to mitigate risk.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The installation of untested patches can result in computers and servers crashing, creating a reliability issue. Moreover, the failure to test or monitor patches could create windows of opportunity to compromise the system.

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

URE1 submitted Mitigation Activities to address the referenced violations. URE1's Mitigating Activities represented that URE1:

1. utilized the current parent company's NERC CIP-007 Compliance Program to design patch management for newly identified Cyber Assets;
2. identified security patch sources;
3. implemented security patch management process; and
4. trained appropriate personnel on the process.

RFC2014013795 CIP-007-3a R3- OVERVIEW

ReliabilityFirst determined that URE2 violated CIP-007-3a R3 by failing to perform patch assessments for third-party applications after commissioning the EMS system. Although the responsible individual was performing operating system level patches at proper intervals based on scheduled tasks, he was unaware of his responsibility to assess third-party patches, which are separate and distinct from those related to the operating system.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The risk was increased due to the EMS being involved in the violation, which increased the risk that the EMS could have been exploited via a vulnerability resulting from an unassessed patch. Furthermore, ReliabilityFirst noted that this violation was not the result of URE2 simply failing to assess two third-party application patches while performing assessments on all other third-party application patches. Rather, this violation was the result of URE2's general lack of awareness to assess third-party application patches.

Nevertheless, ReliabilityFirst notes that the risk posed by this violation was mitigated by the following factors. First, only two security-related patch updates were missed during the period of the violation. Second, all of the operating system level patch assessments for all applicable devices were performed during the period of the violation.

ReliabilityFirst determined the duration of the violation to be from the date that the first third-party patches were not assessed, through when URE2 completed its Mitigation Plan.

URE2 submitted its Mitigation Plan designated RFCMIT011437 to address the referenced violations. URE2's Mitigation Plan required URE2 to provide additional training for responsible personnel on patch assessment requirements.

RFC2014013822 CIP-007-3a R4- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R4 by failing to document the implementation of antivirus and malware prevention tools for cyber assets within the ESP. Moreover, the subsidiary failed to implement a process which addressed testing and installing the signatures for the update of antivirus and malware prevention "signatures."

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The subsidiary's failure to document its anti-virus and malware prevention tools increases the likelihood that it would be unaware of what type or version of these tools it was running. This lack of awareness could result in serious vulnerabilities to subsidiary's cyber security system. The risk posed by the foregoing facts and circumstances was mitigated by the fact that subsidiary had been using undocumented antivirus software and other malware prevention tools for all Cyber Assets within the ESP.

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

URE1 submitted its Mitigation Plan designated RFCMIT011309 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the current parent company's NERC CIP-007 compliance program and associated procedures for change control and commissioning of URE1's Cyber Assets to design configuration of tools to: a) test antivirus signatures prior to roll-out; and b) install antivirus signatures on all applicable Cyber Assets;
2. identify all applicable Cyber Assets for installation of antivirus signatures;

3. ensure that antivirus software has been installed on all applicable Cyber Assets; and
4. train appropriate personnel on the actions necessary for compliance with CIP-007-3a R4.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013823 CIP-007-3a R5- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R5 by failing to: a) document technical and procedural controls that enforce access authentication of, and accountability for, all user activity; b) ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed; c) have designated personnel approve one or more user accounts implemented by the subsidiary; d) review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4; e) implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts; f) for accounts that must remain enabled, change passwords prior to putting any system into service; g) identify all individuals with access to shared accounts; h) where such accounts must be shared, implement (one or more components of) a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination); and i) require passwords subject to R5.3.2 and R5.3.3.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of adequate controls to meet the requirements of CIP-007-3a R5 increases the likelihood that an individual could gain unauthorized access system access and cause serious damage. The risk posed by the foregoing facts and circumstances was mitigated by the logical and physical access controls.

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

URE1 submitted its Mitigation Plan designated RFCMIT011308 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the current parent company's NERC CIP-007 compliance program and associated procedures for change control and commissioning of URE1's Cyber Assets, ensuring that configuration management planning includes processes to: a) baseline all accounts (admin,

shared, service accounts, and generic accounts); b) disable default accounts or change default passwords; c) verify password complexity requirements are met; d) validate access privileges for individuals on the updated CCA access list; and e) ensure traceability of user activity on applicable Cyber Assets;

2. perform initial documentation of its baseline targets for items a) through e) above;
3. implement the parent company's account management process to document account updates for addition of URE1's Cyber Assets; and
4. train appropriate personnel on the actions necessary for compliance with CIP-007-3a R5.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014014469, RFC2014013797, RFC2014013816 CIP-07-3a R5, R5.2.3- OVERVIEW

RFC2014014469

ReliabilityFirst determined that URE2 failed to provide sufficient, or appropriate, evidence to support a valid audit trail of shared, generic, or administrative accounts for the Windows environment. Although URE2 produced sufficient evidence as to who was using generic or shared accounts for other environments (e.g., operating systems and networking devices), URE2 failed to produce any electronic or manual records demonstrating who used the shared or generic account in the operating system environment.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE2 has several procedural controls in place including the current parent company's procedure for acceptable use and definition of the parent's shared accounts, as well as system logs and reviews to track and review when a generic or shared account is used and who has access to use those accounts. Thus, the potential risk associated with not being able to identify which individual is actually using one of these accounts at any given time is minimal.

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

URE2 submitted its Mitigation Plan designated RFCMIT011337 to address the referenced violations. URE2's Mitigation Plan required URE2 to:

1. modify the existing CIP-007 R5 procedure to address appropriate administrative level operating system shared accounts use;

2. modify the CIP-007 R5 training for account use specific to administrator level shared account use and record privileged account users attendance; and
3. implement technical or manual logging of administrative level operating system shared accounts, including an alerting feature for system logging.

RFC2014013797

ReliabilityFirst determined that URE3 violated CIP-007-3a R5 by failing to ensure that all individual and shared system account passwords are changed at least annually. Specifically, the passwords for two service accounts were older than 365 days.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the affected accounts were known to be disabled for interactive login, which reduces the likelihood that these accounts could be compromised. Second, the device at issue is a Cyber Asset for a small group of facilities which rarely run. ReliabilityFirst also notes that an initial evaluation by URE3 indicated that the affected accounts had not been used since creation.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE3 completed its Mitigation Plan.

URE3 submitted its Mitigation Plan designated RFCMIT011424-1 to address the referenced violations. URE3's Mitigation Plan required URE3 to:

1. implement the current parent company's CIP-007 account management procedure to manage built-in accounts when needed;
2. deploy automated scripts to check for passwords nearing the age threshold, verify system password complexity settings and send a report to the site gate keeper; and
3. submit a Technical Feasibility Exception (TFE) for the two system accounts at issue.

RFC2014013816

ReliabilityFirst determined that URE4 violated CIP-007-3a R5 by failing to ensure that all individual and shared system account passwords are changed at least annually. Specifically, three enabled operating system user accounts were found to have passwords older than 365 days.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. First, even though the passwords were not changed in over 365 days, URE4 had other controls in place to physically and logically protect these accounts and devices. Specifically,

these devices resided within an ESP and PSP. Additionally, URE4 generated logs for these devices and accounts to track who accessed them. Second, the devices at issue are Cyber Assets for a small group of facilities which rarely run. ReliabilityFirst also notes that an initial evaluation by URE4 indicated that the affected accounts had been rarely used since their creation.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE4 completed its Mitigation Plan.

URE4 submitted its Mitigation Plan designated RFCMIT011439-1 to address the referenced violations. URE4's Mitigation Plan required URE4 to:

1. implement the current parent company's CIP-007 account management procedure to manage built-in accounts when needed;
2. disable the built-in accounts and then test the functionality of the application; and
3. deploy automated scripts to check for passwords nearing the age threshold, verify system password complexity settings and send a report to the site gate keeper.

RFC2014013824 CIP-007-3a R6- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R6 by failing to: a) implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security on one or more of Cyber Assets inside the ESP in that some of the CCAs within the ESP were missing logs and not all devices within the ESP were accounted for; b) implement and document the organizational processes and technical and procedural mechanisms for monitoring security events on all Cyber Assets within the ESP in that the subsidiary's security monitoring controls do not issue automated or manual alerts for detected cyber security incidents; c) maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008; d) retain one or more of the logs specified in Requirement R6 for at least 90 calendar days without obtaining TFEs for devices that cannot log events; and e) review logs of system events related to cyber security nor maintain records documenting review of logs.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of automated tools or organizational process controls to monitor system events that are related to cyber security increases the likelihood that undetected compromise of CCAs and other system events that are related to cyber security could occur without the subsidiary's knowledge.

The risk posed by the foregoing facts and circumstances was mitigated by the following factors. Although the subsidiary failed to monitor all devices within the ESP for unauthorized cyber or physical access, the GMS, backup GMS, and firewalls were being monitored. Moreover, all Cyber Assets related to the primary and backup GMS were protected by the logical and physical access controls

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

URE1 submitted its Mitigation Plan designated RFCMIT011307 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the parent company's NERC CIP-007 compliance program and associated procedures for change control and commissioning of URE1's Cyber Assets, ensuring that program includes a) processes to monitor all applicable Cyber Assets, including EACMS and PACS; and b) alerting and investigation processes for URE1's Cyber Assets;
2. identify applicable Cyber Assets for security status monitoring, alerting and logging, and to document TFEs as necessary;
3. ensure that security status monitoring, alerting, and log review will be documented and enabled for applicable Cyber Assets; and
4. train appropriate personnel on the actions necessary for compliance with CIP-007-3a R6.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013915 CIP-007-3a R7- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R7 by failing to document the operation and procedural controls to manage the disposal or redeployment of CCAs within the ESP.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The relatively short duration of this violation minimized the likelihood that any data from Cyber Assets could have been retrieved by an unauthorized individual. In addition, URE1 created a technical instruction checklist for disposal of Cyber Assets containing protected cyber information. Furthermore, URE1 does not redeploy Cyber Assets that have been inside the ESPs.

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

URE1 submitted its Mitigation Plan designated RFCMIT011315 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. define the cyber security systems management plan containing operational and procedural controls to manage the disposal or deployment of Cyber Assets within the ESP;
2. implement the cyber security systems management plan; and
3. develop formal documentation of the cyber security systems management plan containing operation and procedural controls to manage the disposal or deployment of Cyber Assets within the ESP and technical instruction for its execution.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013825 CIP-007-3a R8- OVERVIEW

ReliabilityFirst determined that prior to being acquired by the current parent company, the former subsidiary violated CIP-007-3a R8 by failing to perform a CVA, at least annually, of all Cyber Assets within the ESP. An initial CVA did not address all of the sub-requirements of CIP-007-3a R8. Specifically, some devices were not included in the scope of the CVA, and the CVA did not include an action plan to remediate or mitigate vulnerabilities identifying during the CVA and the execution status of that action plan.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The failure to perform a CVA prevented the former subsidiary from identifying inherent vulnerabilities associated with its CCAs. Allowing such vulnerabilities to remain unknown increased the risk that an individual could gain unauthorized access to CCAs within the ESP and caused harm to the integrity of the CCAs. The risk posed by the foregoing facts and circumstances was mitigated by the logical and physical access controls.

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

URE1 submitted its Mitigation Plan designated RFCMIT011318 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. perform a CVA in accordance with the required vulnerability assessment process, review and verify that only ports and services required for operations at these access points are enabled, review controls for default accounts, and document the results of the CVA;

2. develop an action plan for the CVA and document the execution status of that action plan;
3. utilize the current parent company NERC CIP-007 Compliance Program and associated procedures to gather the required information for the CVA;
4. define the scope of work for the CVA that is required to be completed by the end of 2015; and
5. train appropriate personnel on the actions necessary for compliance with CIP-007-3a R8.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013836 CIP-007-3a R9- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R9 by failing to formally define the documentation that would be required for compliance with CIP-007-3. Thus, the subsidiary failed to review, update, or maintain any such documentation.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The violation is a documentation issue. ReliabilityFirst also notes that URE1 identified no known instances where a change to the network or controls was made that would have necessitated a corresponding change in documentation because only minimal system hardware or software changes occurred during the period of this violation.

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

URE1 submitted its Mitigation Plan designated RFCMIT011313 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation of the cyber security systems management program for CIP-007-3a; and
2. implement a formal review and attestation process to ensure that the documentation is updated, reviewed, and maintained to reflect modifications to the systems, configurations, or controls within 30 days of the change.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013826 CIP-008-3 R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-008-3 R1 by failing to document or formally develop a cyber security incident response plan that addressed all of the requisite items. However, the subsidiary had an informal process in place for reporting cyber security incidents, but that informal process lacked the requirements of CIP-008-3 R1.1, 1.2, and 1.6.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk was mitigated because URE1 had an informal process in place for reporting cyber security incidents. ReliabilityFirst also notes that no cyber security incidents occurred during the period of this violation.

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

URE1 submitted its Mitigation Plan designated RFCMIT011217 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation of the measures in place for classifying events, roles and responsibilities for response actions, process for reporting, updating, and ensuring the cyber security incident response plan meets the requirements of CIP-008-3 R1; and
2. formally adopt the cyber security incident response plan for CIP-008-3.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013827 CIP-009-3 R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-009-3 R1 by failing to create a recovery plan for CCAs. Rather, the subsidiary only had an informal, undocumented process in place for the recovery of CCAs.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The lack of a formal, documented recovery plan increases the likelihood that the subsidiary would be unable to recover any failed CCAs. The risk posed by the foregoing facts and circumstances was mitigated by the fact that the subsidiary had an informal, undocumented process in place to recover failed CCAs. ReliabilityFirst also notes that no CCA outages occurred during the period of this violation.

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

URE1 submitted its Mitigation Plan designated RFCMIT011227 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. implement the recovery plan for CCAs as called for by CIP-009-3 R1;
2. develop formal documentation of the recovery plan for CCAs which will contain required actions in response to events and defined roles and responsibilities.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of one hundred and fifty thousand dollars ($150,000) for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors:

1. ReliabilityFirst considered the URE Entities' compliance history as an aggravating factor in the penalty determination;
2. the URE Entities had an internal compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor;
3. the URE Entities self-reported 12 of the violations, and ReliabilityFirst applied some mitigating credit;
4. ReliabilityFirst received a number of the violations as a result of the mandatory Self-Certification process, thus ReliabilityFirst did not provide mitigating credit for the violations during this process;
5. URE1 implemented tools and other measures to enhance the security and reliability of its systems beyond that which is required by the CIP Reliability Standards. ReliabilityFirst has awarded mitigating credit for these measures;
6. the URE Entities were highly cooperative throughout the compliance enforcement process;
7. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
8. ReliabilityFirst considered the risk and harm posed by the URE Entities to the reliability of the BPS as serious or substantial in the aggregate; and

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

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of one hundred and fifty thousand dollars ($150,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 16, 2015 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred and fifty thousand dollars ($150,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

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

Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0682 (216) 503-9207 facsimile bob.wargo@rfirst.org Deandra Williams-Lewis* Director of Enforcement ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0689 (216) 503-9207 facsimile deandra.williamslewis@rfirst.org Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0683 (216) 503-9207 facsimile jason.blake@rfirst.org	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net *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.

Patrick O'Connor* Associate Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0668 (216) 503-9207 facsimile patrick.oconnor@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.	

Conclusion

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

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Gizelle Wray
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
gizelle.wray@nerc.net
(202) 400-3000
(202) 644-8099 – facsimile

cc: Unidentified Registered Entities
ReliabilityFirst