NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

August 31, 2015

VIA ELECTRONIC FILING

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

Re: **NERC Full Notice of Penalty regarding Unidentified Registered Entity,**
FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations discussed in detail in the Settlement Agreement, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE stipulates to the facts in the Settlement Agreement, admits that those facts constitute violations, and has agreed to a monetary penalty of four

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

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

hundred twenty-five thousand dollars ($425,000) and a non-monetary sanction of a Spot Check, in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement. 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 and below.

NERC Violation ID	Standard	Req	VRF/ VSL[4]	Discovery Method[5] Date	Penalty Amount
RFC2013013255	CIP-002-3	R2	High/ High	SR	$425,000
RFC2013013256					
RFC2014014057	CIP-002-3	R3	High/ High	CA	
RFC2014014058					
RFC2014014059					
RFC2014014034	CIP-003-3	R2.3	Medium/ High		
RFC2014014035					
RFC2014014036					
RFC2014014031	CIP-003-3	R4	Medium/ Severe		
RFC2014014032					
RFC2014014033					
RFC2014014028	CIP-003-3	R5.2	Lower/ Severe		
RFC2014014029					
RFC2014014030					

[4] Violation Risk Factor (VRF) and Violation Severity Level (VSL)

[5] Self-Report (SR) / Self-Certification (SC) / Compliance Audit (CA) / Spot Check (SPC) / Compliance Investigation (CI).

NERC Violation ID	Standard	Req	VRF/ VSL[4]	Discovery Method[5] Date	Penalty Amount
RFC2013012765	CIP-003-3	R6	Lower/ Severe	SR	
RFC2014013308	CIP-003-1	R6	Lower/ Severe	SR	$425,000
RFC2014013311					
RFC2014013314					
RFC2014013710	CIP-004-3a	R2	Medium/ Severe		
RFC2014013714	CIP-004-3a	R4	Lower/ Lower		
RFC2014013693			Lower/ Severe		
RFC2014013695					
RFC2014014025	CIP-005-3a	R1.4, R1.6	Medium/ Severe	CA	
RFC2014014026					
RFC2014014027					
RFC2014014054	CIP-005-3a	R2.1, R2.2, R2.4	Medium/ Severe		
RFC2014014055					
RFC2014014056					
RFC2014013312	CIP-005-3a	R2.2	Medium/ Severe	SR	
RFC2014013332					
RFC2014013367					
RFC2014014169	CIP-005-1	R4	Medium/ Severe		
RFC2014014170					
RFC2014014171					
RFC2014014051	CIP-005-3a	R5.1	Lower/ High	CA	
RFC2014014052					
RFC2014014053					
RFC2014013309	CIP-006-3c	R1.1	Medium/ Severe	SR	
RFC2014014048	CIP-006-3c	R1.1	Medium/ Severe	CA	
RFC2014014049					
RFC2014014050					
RFC2014014040	CIP-006-3c	R1.1	Medium/ Severe		
RFC2014014041					
RFC2014014042					
RFC2014013320	CIP-006-3c	R1.6	Medium/ Severe	SR	
RFC2014013326					
RFC2014013333					

NERC Violation ID	Standard	Req	VRF/ VSL[4]	Discovery Method[5] Date	Penalty Amount
RFC2014014044	CIP-006-3c	R1.6.1	Medium/ Severe	CA	
RFC2014014046					
RFC2014014047					
RFC2014014037	CIP-006-3c	R2.2	Medium/ Severe	CA	$425,000
RFC2014014038					
RFC2014014039					
RFC2015014591	CIP-006-3c	R5	Medium/ Severe	SR	
RFC2014013322	CIP-007-3a	R1.3	Lower/ Severe		
RFC2014013327					
RFC2014013334					
RFC2014013335	CIP-007-3a	R2	Medium/ Severe		
RFC2014014072	CIP-007-3a	R2.1, R2.2	Medium/ Severe	CA	
RFC2014014073					
RFC2014014074					
RFC2013012767	CIP-007-3a	R2.2	Medium/ Severe	SR	
RFC2014013310	CIP-007-1	R2.2	Medium/ Severe		
RFC2014013313					
RFC2014013315					
RFC2014013321	CIP-007-3a	R3.1	Lower/ Severe		
RFC2014013328					
RFC2014013336					
RFC2014014078	CIP-007-3a	R3.1, R3.2	Lower/ Severe	CA	
RFC2014014079					
RFC2014014080					
RFC2014013692	CIP-007-1	R4	Medium/ Severe	SR	
RFC2014013694					
RFC2014013696					
RFC2014014069	CIP-007-3a	R4.1, R4.2	Medium/ Severe	CA	
RFC2014014070					
RFC2014014071					
RFC2014014066	CIP-007-3a	R5.1.2, R5.2, R5.2.1,	Medium/ Severe		
RFC2014014067					

NERC Violation ID	Standard	Req	VRF/ VSL[4]	Discovery Method[5] Date	Penalty Amount
RFC2014014068		R5.2.2, R5.2.3			
RFC2014013428	CIP-007-3a	R5.2, R5.3	Lower/ Severe	SR	
RFC2014014009	CIP-007-3a	R5			
RFC2014013323	CIP-007-3a	R5.1.1, R5.1.3	Lower/ Severe	SR	$425,000
RFC2014013329					
RFC2014014008					
RFC2014014063	CIP-007-3a	R6.1, R6.4	Medium/ Severe	CA	
RFC2014014064					
RFC2014014065					
RFC2014013324	CIP-007-1	R6.5	Lower/ Severe	SR	
RFC2014013330					
RFC2014013338					
RFC2014014060	CIP-007-1	R8.2, R8.3	Medium/ Severe	CA	
RFC2014014061					
RFC2014014062					
RFC2014013325	CIP-007-3a	R8	Medium/ Severe	SR	
RFC2014013331					
RFC2014013339					
RFC2014014075	CIP-008-3	R1.6	Lower/ High	CA	
RFC2014014076					
RFC2014014077					
RFC2014013378	CIP-009-3	R5	Lower/ Severe	SR	
RFC2014013379					

OVERVIEW

The Settlement Agreement resolves 102 violations of CIP Reliability Standards.

ReliabilityFirst determined there were several overarching factors that contributed to the violations, including inconsistent processes and procedures across URE functional groups, charging its Information Technology Department (the IT Department) with primary responsibility for CIP compliance, and manual processes that were ineffective and more susceptible to error. URE identified these overarching factors prior to its Compliance Audit and immediately engaged ReliabilityFirst to develop a plan to address them.

URE implemented systematic changes (such as overhauling numerous procedures and adding automation tools) to enhance CIP compliance culture and increase their preparedness for the CIP Version 5 Requirements which become effective on April 1, 2016. To address the underlying root causes of the violations, URE, among other things: 1) moved the CIP compliance function from the IT Department to a different department to help implement and oversee consistent processes; 2) consolidated its CIP policies and procedures–resulting in a 75% reduction in documents used for implementing CIP-related controls; and 3) automated processes where practicable. Through mitigation and above-and-beyond activities, URE increased its maturity in the core management practices of reliability quality management, workforce management, information management, and asset and configuration management. In addition to the strengthening of its compliance functions and subject matter expertise, URE also increased its capacity in the Human Resources Department to support the training of personnel on CIP compliance responsibilities.

CIP-002-3 R2 (RFC2013013255)

ReliabilityFirst determined that URE failed to complete the annual Critical Asset identification process within the required timeframe. Due to an oversight finalizing supporting documentation, the process was delayed by approximately two months.

ReliabilityFirst determined the duration of the violation to be from when URE should have added a substation to its list of Critical Assets, through when URE updated its Critical Asset and Cyber Asset list.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). The substation was on URE's Critical Cyber Asset (CCA) list. In addition, the substation in question was at all times being protected as part of URE's Critical Assets and CIP program. Finally, the duration of the violation was relatively short.

URE's Mitigation Plan (RFCMIT010275) to address this violation was submitted to ReliabilityFirst.

The URE Mitigation Plan required URE to:

1. revise and update its Critical Asset and Cyber Asset lists; and
2. revise its Critical Asset and CCA identification procedures.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the URE Mitigation Plan was complete.

CIP-002-3 R2 (RFC2013013256)

ReliabilityFirst determined that URE failed to complete the annual Critical Asset identification process within the required timeframe. Due to an oversight finalizing supporting documentation, the process was delayed by approximately two months. During the review, the responsible individual identified a change from the initial results in that substations not previously on the Critical Asset list were required to be added to the Critical Asset list.

ReliabilityFirst determined the duration of the violation to be from when URE should have added the substations to its Critical Asset list, through when URE updated its Critical Asset and Cyber Asset list.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had treated the substations at issue as essential assets for several years prior to the violation and they had CIP protections. In addition, the locations have had physical asset controls in place for several years along with electronic access controls to promote the security and reliability of the BPS. Finally, the duration of the violation was relatively short.

URE's Mitigation Plan (RFCMIT010276) to address this violation was submitted to ReliabilityFirst as complete.

The URE Mitigation Plan required URE to:

1. revise and update its Critical Asset and Cyber Asset lists; and
2. revise its Critical Asset and CCA identification procedures.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-002-3 R3 (RFC2014014057, RFC2014014058, and RFC2014014059)

ReliabilityFirst determined that URE failed to develop its lists of CCAs using the lists of Critical Assets developed pursuant to CIP-002-3 R2. The failure related to a relay and Supervisory Control and Data Acquisition (SCADA) Protocol Translator (SPT) terminal servers. The instances of failure were due to the lack of training for the individuals installing Cyber Assets, who failed to follow processes, and a lack of effective asset and configuration management controls. In addition, URE did not have a procedure for adding, removing, or modifying Cyber Assets into the URE CIP environment.

ReliabilityFirst determined the duration of the violations began when URE published a CCA list without the CCA at issue and CCAs were placed into production, through when URE published a corrected CCA list.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because not developing a complete lists of CCAs increased the risk that URE would miss CCAs that were not on the list when implementing the security controls.

The relay was tested prior to implementation and was afforded all of the required security protections and standards for CCAs. Based on the CCA list, there were SPT terminal servers that were re-commissioned and not accounted for on the CCA list. However, the devices did not have external communication capabilities as they were only configured to communicate within the ESP, but not accounted for on the CCA list and not afforded cyber security controls as required by the CIP standards.

URE's Mitigation Plan (RFCMIT011116-1) to address these violations was submitted to ReliabilityFirst.

The URE Mitigation Plan required URE to:

1. complete the commissioning process for the relay and SPT terminal server Cyber Assets and audit the results;
2. review URE processes for the definition of significant change and determine if that covers potential conditions related to the CIP environment. This included how a change in one part of the CIP environment needs to be considered in other parts of the CIP environment;
3. review potential modifications to the URE CIP commissioning and change and configuration management processes for additional refinements with URE personnel who would start the change management process, review and approve the change request, and then execute the changes to the CIP environment;
4. review asset management processes and data to determine if the appropriate Cyber Asset data is maintained over the life-cycle of the Cyber Asset. This would include information on initial purchase, configuration, deployment, modifications, re-deployment, and disposal;
5. interview Subject Matter Experts (SMEs) involved in Cyber Asset commissioning to determine areas of confusion that create inconsistent compliance application and results;
6. review URE processes and tools to remove any potential confusion on execution and capture the recommendations;

7. establish asset management processes and database for all URE functional departments involved with the CIP environment;
8. update or create URE process(es) per the recommended modifications. This will include determination of internal controls to assist in the prevention and detection of conditions which would lead to non-compliance;
9. conduct training for all URE personnel, that work in or affect the CIP environment on the revised and new processes and controls; and
10. review process execution.

URE certified that the above Mitigation Plan requirements were completed.

<u>CIP-003-3 R2.3 (RFC2014014034, RFC2014014035, RFC2014014036)</u>

ReliabilityFirst determined that URE failed to have the CIP senior manager or a designee approve delegations. The violations were due to a lack of effective workforce management controls in not training personnel on the requirement to have the CIP senior manager or designee sign the policies at issue.

ReliabilityFirst determined the duration of the violations to be from when the first document was published without the necessary signature, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Although the CIP senior manager designee was not a signatory to the policy identifying the delegations, an executive, who is involved in URE's compliance program, did review and approve the policy. Senior management had visibility into compliance matters and specifically approved certain delegations, minimizing the possibility of security actions outside of defined and approved processes.

The URE Mitigation Plan (RFCMIT011257) to address these violations was submitted to ReliabilityFirst.

The URE Mitigation Plan required URE to:

1. revise and release a revision of the relevant document signed by the CIP senior manager designate. In addition, URE removed all delegations previously included, except for an emergency successor;

2. host a series of sessions to develop strategies to remediate delegation and designation of the CIP senior manager and associated duties. These sessions involved the CIP-003 Standard owner, director of CIP initiatives, URE information officer and NERC CIP senior manager, along with a third-party compliance consultant;
3. revise the relevant document to only cover the name, title, date of designation, and responsibilities for the assigned CIP senior manager designate;
4. establish and implement a policy document for when the CIP senior manager designate assigns authority to a delegate, or delegates. This new policy document will cover the why, when, and how the CIP senior manager designate will delegate specific authority to a delegate or delegates;
5. distribute informational communication to URE management with distribution of new policy for when the CIP senior manager designate assigns authority to a delegate or delegates. The policy describing the delegation of authority by the CIP senior manager designate will go to the URE management staff that will be on the distribution list for when delegations occur;
6. set-up an electronic distribution list for the CIP senior manager designate to use for distribution of a standardized email communication notifying appropriate URE management of situations in which authority has been delegated for specific actions to named delegate or delegates, for a discrete period of time. The email communication will include the named delegate, or delegates, their titles, contact information, discrete period of time, and the specific actions in which they have been delegated authority; and
7. set up a secure folder with access limited to specific personnel for the storage of the email communications from the CIP senior manager designate.

URE certified that the above Mitigation Plan requirements were completed.

CIP-003-3 R4 (RFC2014014031, RFC2014014032, RFC2014014033)

ReliabilityFirst determined that URE failed to identify, classify, and protect CCA information that resided on third-party hardware. URE failed to consider the protection of CCA information in dealing with the third-party vendor and the contract did not include access provisions or stipulations for how CCA information would be protected.

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

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because URE did not have controls in place to ensure that the third-party vendor was protecting their CCA information housed by the third-party vendor, including internet connection sharing (ICS) devices, names, user IDs, and passwords, which could have exposed the CCA information to unauthorized access. Although information protection was not explicitly documented in the third-party contract, the vendor in question has a high-level of exposure with the CIP requirements, is aware of the necessity to protect URE CCA information, and has a good reputation for maintaining security.

URE's Mitigation Plan (RFCMIT011117-1) to address these violations was submitted to Reliability First.

URE's Mitigation Plan required URE to:

1. create a document requiring information management and protection controls;
2. develop an information management and protection business assessment strategy for all systems, internal and external;
3. revise its information protection program to address protection of CIP information on third-party systems;
4. implement an information management and protection business assessment strategy for all systems, internal and external;
5. complete the execution plan based on the outcome of the information management and protection business assessment of the systems;
6. assess existing CIP environment URE vendor contracts to determine if the appropriate level of information management and protection exists based on the revised and newly created controls;
7. revise existing contract to include information management and protection controls as required by revised URE policies;
8. develop a corporate policy for information management and vendor contract language; and procedure for identifying contracts that require critical energy infrastructure information (CEII) protections and non-disclosure agreements (NDAs);
9. provide training on revised or newly developed information protection plan, policies and procedures;

10. implement a corporate policy for information management and vendor contract language; and procedure for identifying contracts that require CEII protections and NDAs; and
11. perform verification that applicable CIP environment vendors are adhering to the contractual obligations.

URE certified that the above Mitigation Plan requirements were completed.

CIP-003-3 R5 (RFC2014014028, RFC2014014029, RFC2014014030)

ReliabilityFirst determined that URE failed to conduct an annual review of access privileges to protected information, specifically the privileges assigned to access roles in URE's access request and approval system. URE did not have a defined policy or methodology for managing privileges assigned to roles due to the complexity and magnitude of the CIP program outgrowing URE's resources and access management practices.

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

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because not having a thorough annual review including verifying privileges in URE access request and approval system versus actual privileges on devices increased the risk of inadvertent unauthorized access to CCA information. In addition, not maintaining a list of personnel authorizing access to the CCA information areas increased the possibility of granting unauthorized access without the proper approvals. However, URE did review the access lists quarterly, updates, and maintains access in accordance with the results of those reviews. Also, URE had other safeguards in place to protect against unauthorized access to CCA information, such as cameras at the Physical Security Perimeters (PSPs) monitoring access logs.

URE's Mitigation Plan (RFCMIT011258) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. establish business processes to execute and document a complete review and management of URE personnel accesses for all functional groups;
2. perform and document an assessment and evaluation of administrative, technical, and procedural controls of access privileges;

3. create or revise existing processes and methodologies for access control based on the assessment and evaluation results;
4. develop a management process for enterprise-wide job role privilege provisioning and revocation;
5. refine the annual review process to incorporate enterprise roles and all associated access privileges;
6. execute the refined annual review process to review access privileges; and
7. configure the technical tools in place to enhance capturing user and role access, reporting features, and automate review process.

URE certified that the above Mitigation Plan requirements were completed.

CIP-003 R6 (RFC2013012765)

ReliabilityFirst determined that URE failed to publish specific configuration procedures and failed to follow its change control and configuration management process for CIP baseline testing and implementation of interface cards. URE discovered this violation during its Cyber Vulnerability Assessment (CVA).

ReliabilityFirst determined the duration of the violation to be from when URE commissioned and placed the interface cards into service, through when URE disabled the applicable ports.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The devices at issue were non-CCAs inside the Electronic Security Perimeter (ESP) and PSP that only provide an Ethernet-to-serial protocol conversion to allow communication. The protective measures for the ESP, such as the firewall rules and security event monitoring, and the PSP, such as the card access and video monitoring, reduced the risk posed by the non-CCA devices.

URE’s Mitigation Plan (RFCMIT010170) to address this violation was submitted to ReliabilityFirst.

URE’s Mitigation Plan required URE to:

1. create IP ports and services procedure for interface cards; and
2. disable the IP ports for the cards.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the URE Mitigation Plan was complete.

CIP-003 R6 (RFC2014013308, RFC2014013311, RFC2014013314)

ReliabilityFirst determined that URE failed to publish configuration procedures and failed to follow URE change control and configuration management process. Specifically, URE discovered during its CVA that it had enabled unnecessary IP ports on certain Physical Access Control Systems (PACS) due to not changing a factory setting enabling ports not necessary for normal operation.

ReliabilityFirst determined the duration of the violations to be from when URE needed to comply with the Standard, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The PACS devices at issue were non-CCAs inside the ESP and PSP that only provide an Ethernet-to-serial protocol conversion to allow communication. The protective measures of the ESP, such as the firewall rules and security event monitoring, and the PSP, such as the card access and video monitoring, reduced the risk posed by open ports on these non-CCA devices.

URE's Mitigation Plan (RFCMIT011288) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. review and revise the master security configuration to ensure the ports are properly documented;
2. establish a change and configuration committee to align URE functional groups and build commitment, manage CIP environment changes, and enable URE to support the complex process of implementing configuration changes that may affect various functional groups. Establishing and achieving change management objectives helps URE more effectively implement the changes necessary to maintain operations and adhere to compliance requirements. This committee will serve as a formal peer-to-peer information sharing and support forum.
3. revise current URE processes and procedures to include procurement, risk assessment, asset management, supply chain, and testing trigger points, requirements, and hand-offs;
4. conduct training for all URE personnel that work in or affect the CIP environment on the resulting revised and new processes and controls;

5. perform an assessment of current URE software and tools used by all functional groups for change management and configuration controls to determine if there is a single tool or combination of limited tools that can be leveraged and implement accordingly to support URE's CIP compliance program thereby mitigating the number of existing tools URE employs to support change and configuration management; and
6. review process execution.

URE certified that the above Mitigation Plan requirements were completed.

CIP-004-3a R2 (RFC2014013710)

ReliabilityFirst determined that URE failed to ensure that all personnel having access to CCAs were trained prior to being granted such access. URE discovered that certain joint operating company (JOC) personnel had not completed the mandatory annual JOC CIP training. URE notified its corporate security department, which deactivated access cards for the identified personnel. The discrepancies were due to an inaccurate tracking report that had an incorrect field, resulting in URE not reviewing or verifying certain criteria. This in turn was due to ineffective verification and workforce management controls, such as training.

ReliabilityFirst determined the duration of the violation to be from the date when the annual training for the first individual was due to be completed, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because failing to ensure personnel are trained prior to access increases the likelihood that untrained personnel may have cyber or unescorted physical access to CCAs. However, the individuals URE identified for failing to complete the mandatory annual training did timely complete previous training and there were no material changes from the previous training to the missed training. In addition, URE immediately revoked access upon identifying the individuals who did not complete training, and reinstated the access after the individuals completed the appropriate training.

URE's Mitigation Plan (RFCMIT011268) to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. reprimand the administrator responsible for the training system during the time of the described occurrence, make them aware of the issue, and reinforce the training requirements of Standard CIP-004;
2. hire a dedicated resource to centralize the management of the learning management system (LMS). This resource would be responsible for enrollment, tracking, and validating completion of appropriate training, generating and distributing reports, and other duties as required;
3. populate appropriate fields in LMS after performing a manual validation and reconciliation process to determine the extent of conditions, resulting in the creation of a list of active JOC personnel required to take the mandatory annual JOC training;
4. correct the LMS reporting procedure to provide consistent LMS reporting information based on the same criteria used for training enrollment;
5. establish a training enrollment process and procedure for required URE training modules;
6. establish a periodic reporting process to identify when there are [EMPTY or BLANK] fields in LMS user training records; and
7. establish a data integrity auditing process for the LMS user training records.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the URE Mitigation Plan was complete.

CIP-004-3a R4 (RFC2014013714)

ReliabilityFirst determined that URE failed to revoke access to CCAs within seven calendar days for personnel who no longer require such access to CCAs. A URE JOC identified instances involving individuals who retired without the URE JOC collecting their access badges or informing URE to remove their access. The URE JOC also identified an instance in which it had delayed informing URE to terminate a contractor’s physical access to a CIP facility. The failures were due to a lack of effective workforce management controls and training.

ReliabilityFirst determined the duration of the instances to be from the dates URE was required to remove access through the dates it removed access.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, not revoking authorized access upon retirement permits unauthorized access to

CCAs, which could put the BPS at risk. The individuals no longer required access, but URE did not take their access badges upon retirement. Thus, those individuals or anyone who may have had access to those badges could have accessed the CCAs located at critical facilities. Although the employees were trusted employees who completed all of the requirements and training to be granted physical access to CCAs, there was the potential for this same violation to have occurred with other individuals, such as contractors, because of process gaps relating to notice to URE of individuals who no longer require access. In addition, at least for the first instance, it took over two months to notify URE of the first employee's retirement, and discovery only occurred as the result of a quarterly review. Finally, all these instances indicate a programmatic failure related to CIP-004 R4 with similar violations occurring over a three-year period.

URE's Mitigation Plan (RFCMIT011282) to address this violation and violation IDs RFC2014013693 and RFC2014013695, discussed in more detail below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. develop active directory plan for URE's access management system;
2. conduct internal review of JOC access management to develop/revise process to document job role, job function, and business "need-to-know";
3. conduct access management shareholder meeting to review/identify other automated systems for integration into URE's access management system and identify systems that are technically unable to integrate;
4. develop and execute interim process to routinely reconcile URE's access management system approved access to active directory provisioned access;
5. develop integration plan for identified access management systems;
6. develop business process to manage CIP and Non-CIP roles as they are added to URE's access management system to include "need-to-know" business case;
7. engage JOCs to conduct a thorough review of personnel with unescorted physical access and logical access to URE assets, and establish guidelines to implement reviews and increase frequency of reviews;
8. review and revise its procedure to integrate the business process;
9. perform and document an assessment of the current active directory security groups to identify/validate access controllers;

10. complete URE's access management system integration for identified systems;
11. complete update of all active directory security groups and ensure group members have appropriate "need-to-know";
12. configure and enable the URE's access management system reconciliation report to identify discrepancies in access privileges;
13. refine the annual and quarterly review processes to incorporate new business process;
14. establish and implement internal controls for recognition of process execution failures; and
15. conduct training for all URE personnel that work with or affect the access management process resulting from the revised/new processes and controls.

URE certified that the above Mitigation Plan requirements were completed.

CIP-004-3a R4 (RFC2014013693, RFC2014013695)

ReliabilityFirst determined that URE failed to maintain access lists of employees with access to CCAs properly. URE's access management system was unable to demonstrate specific access requests and revocations of sampled personnel with access to IT services within the audit timeframe. This failure was due to ineffective verification controls and insufficient training.

ReliabilityFirst determined the duration of the violation to be from the date URE failed to maintain a list of personnel with authorized cyber or authorized unescorted physical access to CCAs, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because not having an accurate record of access privileges increases the risk of inadvertent unauthorized access to CCA Information. However, although access was not properly recorded, URE confirmed that actual access was maintained and removed as intended for all affected employees and the employees had completed all requirements to be granted access to CCAs.

URE's Mitigation Plan (RFCMIT011282) to address these violations is described in RFC2014013714 above.

CIP-005-3a R1.4, R1.6 (RFC2014014025, RFC2014014026, RFC2014014027)

ReliabilityFirst determined that URE failed to identify certain non-CCAs at URE's control centers within the respective ESPs and failed to identify all ESP access points at URE's control centers. The violation affected Cyber Assets that are used to provide GPS data to establish time values, and redundant firewall Cyber Assets. At the time URE deployed the assets, URE personnel did not understand that all Cyber Assets residing within an ESP must be identified as either a CCA, Electronic Access Control and Monitoring device (EACM), PACS, or Protection Cyber Asset (PCA) even if the Cyber Asset is not directly connected to the ESP internal network.

ReliabilityFirst determined the duration of the violation to be from the last day of the previous URE CIP Compliance Audit, through the date URE updated its documentation to include the GPS data Cyber Assets in the Cyber Asset lists for both control centers.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. First, URE does not consider the GPS data Cyber Assets as essential to the operation of the control center. Second, the GPS data Cyber Assets resided within an ESP and PSP and are not directly accessible from the internet, but rather only locally accessible, and thus were protected from unauthorized access. Third, URE did document the primary firewall physical and logical ports as access points because the primary and secondary firewalls are logically considered as a single Cyber Asset with a single management interface and configuration. Finally, the devices are housed in an identified PSP, which allows only authorized physical access.

URE's Mitigation Plan (RFCMIT011267) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. update the Cyber Asset list to indicate GPS data Cyber Assets within the ESP, and to include the secondary firewall as an Access Point;
2. review URE processes for the definition of "significant change" and determine if it covers all potential conditions related to the CIP environment. This would include when a Cyber Asset is introduced to the CIP environment, how should it be classified if there is redundant hardware or if it is not directly connected to an ESP network, but to Cyber Assets within the ESP, and the overall effect to the CIP environment of those connections;
3. interview and survey SMEs involved in Cyber Asset commissioning to:
    a. assess their understanding of what is a "significant change";

   b. determine what is required for a "significant change"; and

   c. suggest methods to improve processes on identification of "significant change" and how they should be processed.

4. determine how to take into account redundant hardware Cyber Assets and how they should be identified and documented. At a minimum this should indicate how the physical and logical devices and connections should be handled and identified. Information will be used to update the appropriate URE processes to handle this type of "significant change";

5. review URE processes to determine if documentation exists on how to classify Cyber Assets to be introduced to the CIP environment. Classification process should at a minimum indicate how to identify the different Cyber Asset types (i.e. CCA, EACMS, PACS, PCA) and the URE processes that should be executed to make the Cyber Assets compliant with the CIP Reliability Standards;

6. revise processes as deemed necessary;

7. conduct training for all URE personnel, corporate-wide that work with the CIP environment on the revised and new processes and controls;

8. review all ESPs for Cyber Assets not identified within the ESP in a similar condition as the GPS Cyber Assets. Where additional Cyber Assets are identified, complete the necessary documentation as required by CIP-002 through CIP-009, as an additional milestone;

9. determine internal preventative and detective controls for recognition of "significant change" and potential process execution failures. This would be based on the recommended modifications to the URE processes and the process steps to be included for areas of potential errors. Review and determination of internal controls should be completed after process steps are known and their risk for error in execution can be evaluated; and

10. review process execution.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-3a R2.1, R2.2, R2.4 (RFC2014014054, RFC2014014055, RFC2014014056)

ReliabilityFirst determined that URE failed to implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESPs. URE used an overly broad IP address access range space in a firewall rule set such that explicit deny by default was not implemented (R2.1). URE enabled ports on the firewalls that were not justified as required for operations and for monitoring Cyber Assets within the ESP (R2.2). URE did not demonstrate the use of strong procedural or technical controls at the access points (R2.4).

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

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because failure to limit routable communication across the access points to the ESP weakens a layer of defense required for protection of CCAs. However, the broad IP address range communications were restricted to protected networks that were isolated from external CIP environment networks using firewall technology that only allowed necessary in-bound communications. In addition, the unnecessary enabled ports on the firewalls were isolated to the internal protected networks that did not have external communications to networks outside of the protected networks. Finally, although there was a lack of detailed written documentation on the procedural and technical controls in place for remote access to the control center and substation networks, multiple other safeguards were used including user name and passwords as well as firewall protections.

URE's Mitigation Plan (RFCMIT011115-1) to address these violations and violation IDs RFC2014013312, RFC2014013332, RFC2014013367, discussed in more detail below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. disable identified unnecessary enable ports for occurrences mentioned and update required documentation;
2. review all electronic access points in the URE environment to verify only ports and services required for operation are enabled and are documented;
3. develop documented process that enables validation of information on the change orders (exceptions);
4. complete review of change management for communications with all relevant CIP environment groups;
5. review the potential modifications to the URE change management processes for additional refinements with URE personnel who would start the change management process, review and approve the change request, and then execute the changes to the CIP environment;

6. complete update of change management and change order processes;

7. complete training of all URE personnel involved in the change management and change order processes;

8. complete review of modified change management and change order processes, and identification of areas for improvement including process updates;

9. complete process for collection of IP address/port matrix for use in elimination of broad IP address/port access controls for control center and substation network communications;

10. complete modification of control center and substation network communications;

11. complete creation of detailed procedural and technical controls documentation for control center and substation network communications;

12. complete investigation and approval for multi-factor authentication for remote access;

13. complete implementation of multi-factor authentication for remote access;

14. complete creation of detailed procedural and technical controls documentation for multi-factor authentication; and

15. complete training of applicable URE personnel on multi-factor authentication for remote access.

URE certified that the above Mitigation Plan requirements were completed.

<u>CIP-005-3a R2.2 (RFC2014013312, RFC2014013332, RFC2014013367)</u>

ReliabilityFirst determined that URE failed to enable only ports and services required for operations and failed to document accurately the configuration of its ports. This failure was due to ambiguous language in a related change request. In addition, URE's change spreadsheet did not match the actual configuration of several firewalls at URE's control centers. The documented change management procedures in place at the time did not include instructions on communicating changes with the IT department or verifying that the documentation of required configurations were updated.

ReliabilityFirst determined the duration of the violations to be from the date the port documentation was validated as part of the CVA process, through the date URE disabled the unnecessary ports and updated the documentation to reflect accurate configurations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The erroneously enabled port was only for communications between the control houses and there were no communication capabilities in or out of the ESP. Therefore, someone would first have to get through safeguards surrounding the ESP, such as firewalls, before being able to access information through the enabled port. The actual configuration of the firewalls had the correct enabled ports that were required for operations, and the change management documentation had the correct modification information, but the IT department's change spreadsheet was incorrect.

URE's Mitigation Plan (RFCMIT011115-1) to address these violations is described in RFC2014014054, RFC2014014055, and RFC2014014056 above.

CIP-005-1 R4 (RFC2014014169, RFC2014014170, RFC2014014171)

ReliabilityFirst determined that URE failed to verify, during their CVAs, that only ports and services required for operations at access points were enabled. URE discovered a port that allowed access to the ESP at multiple access points that was not required for normal operations. URE should have discovered this port during its previous CVAs.

ReliabilityFirst determined the duration of the violations to be from the date URE was required to comply with CIP-005 R4, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because undocumented ports and services potentially permit unauthorized access to Cyber Assets within an ESP and lack of awareness to review ports and services required for operations at the access points cause exploitable security weaknesses. However, the risk was mitigated because the unnecessary enabled port and service in this instance allowed communications into the ESP to Cyber Assets that were no longer configured to allow connections for the enabled port/service. Therefore, even if an intruder gained access into the ESP through the enabled port, the intruder could not actually obtain information related to CCAs, but could potentially exploit the access point.

URE's Mitigation Plan (RFCMIT011266) to address these violations was submitted to ReliabilityFirst.

URE’s Mitigation Plan required URE to:

1. update baseline documentation to include "listening" ports as well as "established" ports/services information;
2. complete review and update of policies and process on required ports/services information;
3. complete review and update of policies and process on what is required for account controls;
4. complete determination of collection method for ports/services information;
5. complete training for all URE personnel on required ports/services and account information and maintenance;
6. complete review and update of the CVA process for establishment of ports/services data, collection of the data, comparison of the data, internal controls to help detect abnormal conditions, and the processes cover all of the CIP requirements;
7. complete execution of the updated CVA process including review of baseline data used for the CVA process to verify the data reflects current operational conditions; and
8. correct the baseline data for instances discovered where the baseline data did not reflect current operational conditions.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-3a R5.1 (RFC2014014051, RFC2014014052, RFC2014014053)

ReliabilityFirst determined that URE failed to ensure its documentation reflected current configurations and processes. The affected assets included GPS data Cyber Assets and ESP access points. The failures were due to a lack of understanding of the CIP requirements for Cyber Asset identification.

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE updated its documentation to include the GPS data Cyber Assets in the Cyber Asset lists for both control centers.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The GPS data Cyber Assets are not considered essential to the operation of the control center, resided within an ESP and PSP, are not accessible directly from the internet, but rather only locally accessible, and are therefore protected from unauthorized access. In addition, URE did document the primary firewall physical and logical ports as ESP access points and housed them within an identified PSP

URE’s Mitigation Plan (RFCMIT011265) to address these violations was submitted to ReliabilityFirst.

URE’s Mitigation Plan required URE to:

1. update ESP drawing, CCA list and associated documentation (CIP-002 through CIP-009) to include GPS data Cyber Assets and Access Points;
2. complete review of URE processes for “significant change”;
3. complete SME interviews and surveys concerning the commissioning processes;
4. issue URE ruling on handling of redundant hardware Cyber Assets;
5. complete review of URE processes used for determination of Cyber Asset classification;
6. revise URE processes used for determination of Cyber Asset classification;
7. complete training of all URE personnel involved in the introduction of Cyber Assets to the CIP environment on the revised URE processes;
8. complete review of all ESPs to identify Cyber Assets that were not previously identified, classified, and/or documented;
9. update URE Cyber Asset lists, diagrams, and associated documentation (CIP-002 through CIP-009) to reflect newly identified Cyber Assets; and
10. develop and implement internal controls to prevent and detect process failures.

URE certified that the above Mitigation Plan requirements were completed.

<u>CIP-006-3c R1 (RFC2014014040, RFC2014014041, RFC2014014042)</u>

ReliabilityFirst determined that URE failed to provide the protective measure to a substation radio transmitter system pairs to justify a Technical Feasibility Exception (TFE) under CIP-006 R1.1. The TFE at issue identified a compensating measure requiring the protective measure of encryption on the substation radio transmitter system pairs. However, URE did not enable encryption on the pairs.

ReliabilityFirst determined the duration of the violations to be from the date substation radio transmitter pairs went into production, through the date URE enabled encryption on the devices.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Although encryption was not enabled, the fact that remote access was disabled only permitted local access to the devices. The protective measures surrounding the devices, such as an actively monitored PSP and ESP, mitigated the risk of someone gaining unauthorized access to the devices.

URE's Mitigation Plan (RFCMIT011264) to address these violations, and the violations of RFC2014014044, RFC2014014046, RFC2014014047, RFC2014014048, RFC2014014049, RFC2014014050, RFC2014013320, RFC2014013326, and RFC2014013333 described below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. notify URE corporate security executives and management of incident;
2. perform an investigation and interview individuals involved in granting unauthorized physical access;
3. determine and levy disciplinary action against offender;
4. update all PSP URE visitor logbooks with instructions for completing all fields;
5. train offender on CIP access requirements;
6. develop URE visitor and escort training curriculum;
7. notify URE employees, JOCs, and contractors of mandatory URE visitor and escort training;
8. secure cable trays and close all PSP openings more than six inches within operations control rooms;
9. enable encryption on radios;
10. prepare lessons learned from configuration of radios;
11. develop control center physical security inspection;
12. inspect PSP boundaries to ensure CCAs, Non-critical Cyber Assets, and ESPs are within a six-wall boundary;
13. update testing and approval of hardware, firmware and software for CCA devices procedure to ensure TFEs are addressed;
14. develop process for inspecting and correcting URE visitor logbooks entries;

15. place cabinet visitor logbooks in every cabinet PSP; and
16. perform random sample spot-check of newly implemented processes and logbooks;

URE certified that the above Mitigation Plan requirements were completed

CIP-006-3c R1 (RFC2014014044, RFC2014014046, RFC2014014047)

ReliabilityFirst determined that URE failed to have visitor logs for certain cabinets, which are identified PSPs. Technicians were required to contact the control room prior to opening a cabinet, after which the entrance door is unlocked. URE used an electronic lock system to log approved unescorted access, but did not have a separate log within the cabinets themselves.

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE put visitor logs into the cabinets.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The risk was mitigated because the cyber locks on the cabinets can be opened only by an individual with an electronic lock system key and unescorted physical access into the PSPs. Therefore, visitors cannot enter the PSP without the assistance of an individual with unescorted access and would be logged as a visitor if they were working on the cabinets.

URE's Mitigation Plan (RFCMIT011264) to address these violations is described in RFC2014014040, RFC2014014041, and RFC2014014042 above.

CIP-006-3c R1 (RFC2014014048, RFC2014014049, RFC2014014050)

ReliabilityFirst determined that URE failed to establish a six-wall border throughout the PSP and failed to document all alternative measures that were in place to secure the PSP. There was an opening in the PSP of URE's operations control room that had a cable tray that ran under a cement floor hallway and connected to a non-PSP room on the other side of the hallway. The non-PSP room had drywall covering the opening on that end, however there was no seal to the cable tray opening on the PSP side.

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

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The operations control room, an identified PSP, has staffing 24 hours a day, seven days a week and the floor panels are difficult to penetrate as they are secured. In addition, the non-PSP location adjacent to the PSP has access controls in place.

URE's Mitigation Plan (RFCMIT011264) to address these violations is described in RFC2014014040, RFC2014014041, and RFC2014014042 above.

CIP-006-3c R1.6 (RFC2014013320, RFC2014013326, RFC2014013333)

ReliabilityFirst determined that URE failed to log all required information relating to visitors and failed to have the designated individual provide continuous escorted access to certain visitors. There were instances where details such as time in, time out, or reason for visit were missing in the URE visitor logbooks. Additionally, a JOC employee allowed subcontractors access into the URE control house and then left the visitors in the control house PSP without an official escort.

ReliabilityFirst determined the duration of the violation to be from the first date the logbook entries were incomplete, through when URE completed its mitigation activities for these violations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. In the nine instances identified, the visitors' names were in the visitor logbooks and there is no indication that the individuals were not escorted. Although the official JOC escort did not stay with certain visitors, there were unofficial escorts with the individuals, thus reducing any risk that the individuals could use equipment in a way that would put the BPS at risk or allow access to confidential information.

URE's Mitigation Plans (RFCMIT010968 for RFC2014013320, RFCMIT010966 for RFC2014013326, and RFCMIT010967 for RFC2014013333) to address these violations were submitted to ReliabilityFirst. In addition to these Mitigation Plans, certain mitigation activities taken as a part of RFCMIT011264, described in RFC2014014040, RFC2014014041, and RFC2014014042 above, also mitigated these violations.

URE's Mitigation Plan required URE to:

1. develop training for visitor log book usage;
2. notify JOCs of the mandatory training; and
3. conduct training with URE employees and contractors.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-3c R1 (RFC2014013309)

ReliabilityFirst determined that URE failed to have all Cyber Assets within an identified PSP with an enclosed border. Cabling for the ESP between the PSPs at a URE substation was not inside an encased conduit nor was it inside a controlled six-wall protection boundary.

ReliabilityFirst determined the duration of the violation to be from the date URE needed to comply with the Standard, through when URE installed conduit encasing wiring between the PSPs.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The risk was mitigated because the PSPs at issue were close in proximity in a single URE building that was enclosed with a fenced boundary, and thus there were barriers in place to protect the cabling from intruders.

URE's Mitigation Plan (RFCMIT010804) to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. install conduit encasing wiring between the two PSPs; and
2. publish its substation inspection process document and distribute to key stakeholders and SMEs.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-006-3c R2.2 (RFC2014014037, RFC2014014038, RFC2014014039)

ReliabilityFirst determined that URE failed to provide sufficient evidence that the virtual machine hosts and virtual machine chassis were afforded the protective measures identified in CIP-006-3c R2.2. URE properly identified virtual machines containing PACS applications as PACS with all the appropriate protection controls, however, the virtual machine host running the virtual machine clients were not identified as PACS. The virtual machine host is an integral part of the client and must be afforded the measures as required by the Standard. The failure was due to a lack of training and knowledge on the Standard and requirement.

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

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE did not implement all of the protective measures on the virtual machine hosts as required by CIP-006-3c R2.2, there were multiple other protective measures in place that reduced the risk of unauthorized access to the virtual machine hosts. For example, the virtual machine hosts were inside a PSP with multiple layers of firewalls protecting the hosts; URE performed patching on the hosts and hardware; URE monitored the hosts for operational and security alarms; and all individuals having access to the virtual machine hosts were vetted in accordance with CIP-004 R3.

URE's Mitigation Plan (RFCMIT011283) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. complete review of corporate policies on virtual machines usage and how it applies to the CIP environment;
2. complete catalog of existing virtual machines usage in the CIP environment;
3. complete creation of migration plan if required to separate CIP and non-CIP virtual machines clients;
4. complete development of standard for virtual machines usage in the CIP environment;
5. complete review of change management process for modifications related to virtual machines usage;
6. complete interviews with SMEs, Standard owners, and IT infrastructure on process and standard modifications for virtual machines technology;
7. complete creation and/or update of URE CIP program policies, standards, and processes to ensure compliance of virtual machines technology;
8. train personnel on updated policies, standards, and processes;
9. modify designs to virtual machines technology usage if required to separate virtual machines clients.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-3c R5 (RFC2015014591)

ReliabilityFirst determined that URE failed to review immediately and handle unauthorized access attempts in accordance with the procedures specified in CIP-008-3. An employee of a URE JOC arrived at a URE substation and attempted access to the switchyard by using the JOC-issued access badge. The badge created an alarm that was reported to the URE security command center. The employee then used an issued electronic key system to gain access to the control house twice, although the key was not programed for the substation and therefore set off an alarm. The control house door lock was defective and allowed enough movement when turned in concert with the electronic key system to allow the door to be opened. Once inside the control house, the employee failed to complete all the required fields of the logbook. The employee remained in the control house for eight minutes, exiting and remaining within the switchyard for approximately 30 minutes. URE security officers acknowledged the alarms, determined they were caused by a JOC employee, and failed to investigate the matter further.

ReliabilityFirst determined the duration of the violation to be from the date the URE failed to respond immediately to the alarm conditions, through when URE completed investigation of the alarm conditions.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Even though there were security alarms, URE security personnel did not timely investigate the alarms and conduct due diligence as required by CIP-006-3c R5. Permitting someone without authorized access to access a PSP puts the BPS at risk of that individual tampering with equipment or compromising CCA information in a way that could harm the reliability of the BPS. The security officer immediately recognized the alarms, and thus was aware that the individual was accessing the PSP. In addition, the employee was an active employee, in good standing, with unescorted physical access into URE non-CIP substations, thereby reducing the likelihood that he would have used the access in a way to put the BPS at risk. Finally, during the investigation of the alarms, URE's IT department performed an inspection of the network and identified no abnormalities.

URE's Mitigation Plan (RFCMIT011409) to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. interview, reprimand, and counsel the URE on-duty security officer;
2. conduct an internal thorough investigation of the response to the alarm;

3. disseminate an awareness and training communication and follow-up correspondence reiterating the alarm process and addressing additional inquiries and points of clarification to all personnel at the security command center concerning the incident;
4. replace the locking mechanism on the door latch;
5. complete the review and update (if necessary) its physical access process to ensure the accuracy of its directives for alarm investigations and responses;
6. begin an extent of conditions system-wide inspection, assessment, and test to determine if there were any additional defective locking mechanisms at other URE substations; and
7. complete the training on its physical access process for all its security personnel responsible for the monitoring of URE's physical security system.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R1.3 (RFC2014013322, RFC2014013327, RFC2014013334)

ReliabilityFirst determined that URE failed to document test results for changes or new Cyber Assets. URE did not complete a control and configuration management work form for certain physical security Cyber Assets after reclassifying an URE substation from a non-CIP site to a CIP site, and therefore failed to document test results for the new Cyber Assets introduced into a CIP environment. In addition, URE replaced some existing terminal servers that required the use of terminal servers. The personnel installing these assets did not correctly view the replacement as a significant change to the CIP environment. Finally, URE installed new servers-based Cyber Assets that utilized non-approved versions of one application. URE assigned the task for updating the system version but the assigned team never completed the upgrade, and therefore URE personnel did not verify the version in URE's patch version control document.

ReliabilityFirst determined the duration of the violations to be from the date the first Cyber Assets were commissioned, through when URE updated the application to the correct version, conducted testing, and provided documentation as required by URE processes.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. Specifically, the risk was increased because the newly commissioned Cyber Assets may have caused system instabilities when the new Cyber Assets are placed into production without adequate testing. This may have caused unforeseen vulnerabilities, such as unnecessary open ports or lack of patches or ineffective antivirus software.

URE's Mitigation Plan (RFCMIT011280) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. complete the Cyber Asset commissioning process for the terminal servers;
2. update the application to the correct version, conduct testing and provide documentation as required by URE processes;
3. create and distribute a survey for suggestions on improving process flow and execution;
4. interview SMEs involved in Cyber Asset commissioning to provide feedback and enhancements for the process(es) being developed;
5. review URE processes for the definition of "change" and "significant change" and revise to cover potential conditions, including "like-for-like" replacements, related to the CIP environment;
6. assess URE processes and procedures to include procurement, risk assessment, asset management, and supply chain trigger points and hand-offs to the testing process;
7. create guidelines for defining and documenting the non-production test environment used for CIP-007 R1 significant change testing;
8. revise URE processes and procedures to remove any potential confusion on execution and capture the recommendations from the SME interviews and survey that add-value and provide efficiency;
9. create internal preventative and detective controls for recognition of "significant changes" and actual process execution failures; and
10. conduct training for all URE personnel that work in or affect the CIP environment on the resulting revised and new processes and controls.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3 R2, R2.1, R2.2 (RFC2014013335, RFC2014014072, RFC2014014073, RFC2014014074, RFC2013012767, RFC2014013310, RFC2014013313, RFC2014013315)

ReliabilityFirst determined that URE failed to ensure that only ports and services required for normal or emergency operations were enabled and/or that other ports and services were disabled on Cyber Assets within the ESP prior to production.

During URE's CVA, it discovered an undocumented port and service enabled on a relay and that its ports and services documentation for the Windows systems in the entire CIP environment did not address the required services running on the Cyber Assets without listening ports. URE also discovered an open port and associated service on an Ethernet switch at a transmission substation.

ReliabilityFirst determined the duration of these violations to be from the last day of the previous URE CIP Compliance Audit, through when URE completed its Mitigation Plan.

URE installed modules into the CIP environment with default IP ports enabled. At the time, URE did not have a documented baseline of required ports and services. The enabled IP ports were identified during the CVA, however it did not specify that the review of the enabled ports and services against documentation of required ports and services was applicable to the Cyber Assets.

ReliabilityFirst determined the duration of these violations to be from the date URE needed to comply with the Standard, through when URE completed its Mitigation Plan.

URE discovered an enabled port between a remote terminal unit (RTU) and the annunciator at a URE substation that was not required for operation of the two devices. In addition, during the CVA, URE discovered that a port was enabled on several wireless radios that connect transformer monitoring systems from the substation yard back to the control building. This port was not required for operation of the radios.

ReliabilityFirst determined the duration of these violations to be from when URE enabled the unnecessary ports on the radios, through when URE completed its Mitigation Plan.

URE conducted CIP baseline testing and implementation of an interface card. URE determined the card came configured from the factory with IP ports enabled that are not necessary and should have been disabled prior to installation.

ReliabilityFirst determined the duration of this violation to be from when URE commissioned and placed into service the interface card with unnecessary enabled ports, through when URE disabled the ports.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, URE's not ensuring that it enabled only ports and services required for normal or emergency operations across relays, systems, annunciators, PACS, switches and interface card devices indicated a programmatic failure. In addition, these issues cumulatively create vulnerabilities that expose the systems to a higher risk of compromise by potentially allowing more channels for undetected access into URE's critical systems. Finally, insufficient documentation of the required ports and services on essential Cyber Assets can result in not ensuring only required ports and services are enabled. Given these risks from multiple issues and the duration, the violations posed a serious and substantial risk to the reliability of the BPS.

Due to the timing of the Self-Reports, URE's Mitigation Plan (RFCMIT010171) to address the violation of RFC2013012767 was submitted to ReliabilityFirst prior to the Mitigation Plan addressing the remaining violations in this section.

URE's Mitigation Plan required URE to create an IP Ports and Services procedure for the specific Cyber Asset type and disable the unnecessary ports on the Cyber Assets.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the URE Mitigation Plan was complete.

URE's Mitigation Plan (RFCMIT011278) to address the violations of RFC2014013335, RFC2014014072, RFC2014014073, RFC2014014074, RFC2014013310, RFC2014013313, and RFC2014013315 was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. correct the identified unnecessary enabled ports and services which should have been disabled and update appropriate documentation;
2. review TFEs currently in place to ensure they accurately represent URE's Cyber Asset capabilities;
3. submit or revise TFEs currently in place to address any misrepresentation of URE's Cyber Asset capabilities;
4. conduct SME interviews for all functional groups involved with Cyber Asset commissioning and vulnerability assessments to improve process flow and execution;
5. conduct a thorough review of all URE Cyber Assets within the CIP environment to verify that only the ports and services required for normal operation are enabled and the documentation of the required ports and services is correct for all devices in the CIP environment. URE would then correct the identified unnecessary enabled ports and update of the appropriate documentation;

6. review and update the processes for Cyber Asset commissioning and vulnerability assessments based on feedback from the interviews with the SMEs from all functional groups and train all URE personnel involved in the Cyber Asset commissioning and vulnerability assessments on the process changes; and
7. review process execution.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R3.1, R3.2 (RFC2014013321, RFC2014013328, RFC2014013336, RFC2014014078, RFC2014014079, RFC2014014080)

ReliabilityFirst determined that URE failed to perform an assessment of security patches and security upgrades within 30 days of availability for all Cyber Assets within the ESP and failed to document the implementation of security patches for all Cyber Assets within the ESP.

URE did not evaluate security patches for the transmission management system's (TMS) servers within the 30-day timeframe. In addition, during a mock audit, URE discovered additional security patches for multiple Cyber Assets were not evaluated within the 30-day required timeframe.

URE also discovered that the PACS Cyber Assets installed with the cyber audit web application did not have patching capabilities as required by CIP-007-3a R3 and URE failed to file a TFE for those assets and failed to document compensating measures. URE had also placed terminal servers into production without the ability to implement patches and that did not have the capability for patching without being set back to the original equipment manufacturer. URE should have created and filed a TFE and compensation controls for these servers.

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

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because failing to timely assess and implement security patches, especially on critical systems, can lead to increased vulnerability to a cyber-attack that could compromise the BPS. However, URE had compensating controls in place while the Cyber Assets were not patched, or where systems could not be patched. These compensating controls included regular monitoring of the systems, with the logs reviewed on a daily basis, and automated alerts for predefined conditions such as excessive login failures of two or more within a short period.

URE’s Mitigation Plan (RFCMIT011263) to address this violation was submitted to ReliabilityFirst.

URE’s Mitigation Plan required URE to:

1. file necessary TFEs for SPT and PACS affected systems;
2. document all applicable operating system and application vendors and their associated patch release schedules and sources;
3. upgrade relevant corporate security PACS servers with the web application to an operating system and application version that supports security patching;
4. develop internal controls to assist in verification of proper process execution with emphasis on preventative controls to catch processing errors at the time of execution;
5. review and update URE policies, processes, and procedures regarding patching to ensure compliance with CIP-007-3 R3. The updated policies, processes, and procedures will:
    a. indicate that original equipment manufacturer sources that should be used for notification of patch releases;
    b. indicate that a 30-day timeframe is required for patch evaluation after original equipment manufacturer release;
    c. address third-party supplier situations;
    d. require inclusion in evaluation documentation the purpose of the patch (i.e. security fix or new features), the applicability, and any effect identified as a result of patching; and
    e. require recommendations within 30 days of the patch evaluation to the asset owner(s).
6. implement a process to indicate source of security patches enforcing that the start of the 30-day timer will be the original equipment manufacturer security patch release date for Cyber Assets within the CIP environment;
7. create a patch evaluation, testing, and deployment schedule to reduce the patch cycle from six months to 90 days;
8. place applicable systems under URE patching process for correct evaluations and installation;
9. provide training to ensure that URE personnel responsible for patch evaluation are aware of original equipment manufacturer patch sources and receive notification of new patch releases and provide training to all URE personnel involved in patching for the CIP environment on all created and revised policies and processes; and

10. verify correct execution of patching.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R4, R4.1 (RFC2014013692, RFC2014013694, RFC2014013696)

ReliabilityFirst determined that URE failed to document compensating measures. While preparing for its Compliance Audit, URE discovered its PACS Cyber Assets that were installed with the web application did not support malware protection software as required by CIP-007 R4. URE had not filed for a TFE or documented compensating measures for these PACS Cyber Assets. In addition, URE discovered SPT terminal servers it had placed into production without applying malware prevention software.

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

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE did not document compensating measures, mitigating measures were implemented during commissioning of the PACS Cyber Assets. Physical and cyber access to the PACS Cyber Assets is limited, along with full logging enabled, for significant events such as login attempts and failures. Ports and services are controlled by the corporate firewall access control lists. The PACS Cyber Assets reside on a secure and separate virtual local area network. The SPT terminal servers did not have external communication capabilities since they were configured to only communicate within the ESP, thereby reducing the possibility of a compromise.

URE's Mitigation Plan (RFCMIT011262) to address these violations, as well as for the violations RFC2014014069, RFC2014014070, and RFC2014014071 discussed below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. review the need for and file necessary malware TFEs for SPTs and PACS;
2. upgrade systems to an operating system and application version that will support malware prevention software;
3. conduct SME interviews to gain insight and solicit recommendations to improve malware signature processing;

4. review all URE policies, processes, and procedures regarding malware protection and revise to indicate clearly malware protection is required for the CIP environment along with requisites of installation and testing of applied signatures, or that a TFE and mitigating protections are required;
5. establish and implement internal controls to verify malware protection is applied to all Cyber Assets that have the capabilities, malware signatures are applied within the prescribed timeframe, and compensating controls are in place;
6. provide training on new or revised processes to all URE personnel involved with malware protection; and
7. conduct review process execution.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R4, R4.2 (RFC2014014069, RFC2014014070, RFC2014014071)

ReliabilityFirst determined that URE failed to document compensating measures for PACS Cyber Assets, and failed to document or implement a process to update antivirus and malware prevention "signatures". URE was unable to provide evidence regarding the testing of malware prevention software signatures as required by CIP-007 R4.2.

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

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The risk was mitigated because although URE could not provide malware signature update documentation, they have the processes and procedures in place for the testing and installation of signature files on Cyber Assets, and indicated that signatures were updated per the current process.

URE's Mitigation Plan (RFCMIT011262) is discussed with violations RFC2014013692, RFC2014013694, and RFC2014013696 above.

CIP-007-3 R5.1.2, R5.2.1, R5.2.2, and R5.2.3 (RFC2014014066, RFC2014014067, RFC2014014068)

ReliabilityFirst determined that URE failed to produce logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of 90 days. In addition, URE failed to have documentation for a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges.

Specifically, URE could not demonstrate sufficient detail on account activity for a sample size of Cyber Assets or provide implementation of a policy and management of shared and default accounts for PACS or the account used by the TMS department. URE did not have information for shared administrator accounts related to electronic lock PACS, could not provide documentation for a policy that includes the removal, disabling, or renaming of shared accounts, and did not provide documentation identifying individuals with access to shared accounts. Finally, URE could not provide documentation that explicitly identifies a policy for managing the use of shared accounts that limits access to only those with authorization, or an audit trail of the account usage and maintenance.

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

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. Specifically, the violations span across multiple systems and accounts in URE's network and inadequate audit trails of user actions on CCAs can lead to missing cyber security events and inadequate shared account management can lead to inadvertent use of URE's CCAs, which can result in compromise of CCAs.

URE's Mitigation Plan (RFCMIT011281) to address these violations, and violations RFC2014013428, RFC2014014009, RFC2014013323, RFC2014013329, and RFC2014014008 discussed below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. file appropriate TFEs for the SPT terminal servers;
2. correct default password configurations on the affected devices;
3. update the account information of URE personnel with knowledge of the accounts;
4. review all processes used the by URE departments for account management to determine how the processes satisfy CIP-007-3a R5 and identify in the processes;
5. review all tools used by URE departments for account management to determine how the tools satisfy CIP-007-3a R5, CIP-003-3 R4, and CIP-003-3 R5 and determine if there are gaps in the toolsets;

6. conduct SME interviews for input on current process execution, problems with the execution, and suggestions on process improvements;
7. create standardized processes across departments;
8. identify standardized tools to handle the account management processes;
9. develop internal controls to identify process execution exceptions, escalation of the exceptions for proper handling, identification of new process requirements, and continuous improvement of the process, and methods to enable adherence to process requirements and consequences for failure to follow the processes;
10. identify and review the usage and documentation of default, root, administrator, and shared accounts in the URE departments for account management and determine how the use of these accounts can be suspended by implementing other accounts, or document special account usage and controls per CIP-007-3a R5.1 and R5.2;
11. review methods used by the URE departments for account management for documenting and recording account usage per CIP-007-3a R5.1.3 and R5.2.3. Where activity usage account is not documented or recorded in sufficient detail, URE would develop methods to collect the information. In instances where the account cannot be disabled, URE would create the necessary documentation capturing the vendor limitations and compensating controls to maintain awareness of account usage;
12. conduct training for URE personnel in the URE departments for account management on the standardized processes and tools; and
13. review process execution item.

URE certified that the above Mitigation Plan requirements were completed.

<u>CIP-007-3a R5 (RFC2014013428, RFC2014014009, RFC2014013323, RFC2014013329, RFC2014014008)</u>

ReliabilityFirst determined that URE failed to implement and document technical and procedural controls that enforce access authorization of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

While preparing for its CIP Compliance Audit, URE discovered several incomplete workforms. URE personnel did not correctly document information on the workforms because URE process documentation was unclear (First Instance). In addition, URE discovered that it did not have sufficient evidence to validate system level access privileges of user accounts on an annual basis. The evidence did not demonstrate that the URE accounts being reviewed were actually checked against the systems on which the accounts were provisioned to ensure the accounts existed and were provisioned correctly (Second Instance). URE also discovered that during its system transition from a corporate security portal to URE's access management system, some of the roles and perimeters were lost from personnel profiles. As a result, when an individual was terminated, there access privileges were not documented as revoked although actual access was revoked (Third Instance).

During its CVA, URE discovered that for two of three shared accounts, passwords and usernames on four Ethernet switches that were inadvertently reset to the factory default usernames and passwords. The passwords were not strong or meet the requirements of CIP-007 R5 (Fourth Instance). In addition, URE discovered that default passwords were on several relays at URE substations—in each device, one shared account was configured with the factory default password and these default passwords were not strong and did not meet URE's Cyber Asset password policy (Fifth Instance).

Finally, URE discovered that SPT terminal servers were placed into production without the application of URE processes for account management. URE also did not request a TFE for these assets. URE personnel did not view the replacement of the assets as a "significant change" to the CIP environment and therefore did not assess, classify, or commission the SPT terminal servers as CCAs (Sixth Instance).

ReliabilityFirst determined the duration of the violations to be from the date the oldest asset at issue was commissioned, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because the failure to implement and document technical and procedural controls that enforce access authentication of all user activity increases the risk of unauthorized access and thus potential compromise of CCAs.

The risk was mitigated for the following reasons. Regarding the First Instance, URE properly configured and recorded the actual account, but URE did not have a complete workform as required by their processes. Regarding the Second Instance, the accounts were in fact provisioned correctly and URE's defense-in-depth strategies reduced the risk of someone accessing the systems for improper purposes. Regarding the Third Instance, logical access was removed from the Cyber Assets. Regarding the Fourth Instance, the Ethernet switches did not have external connectivity or remote management connectivity to allow for potential compromise. Regarding the Fifth Instance, the default passwords were in the upper access tier of the relays, thus someone would have to first use a password for the lower tier to gain access, and the lower tier password was strong. In addition, access to the relays required physical access, which was protected by a PSP. Finally, regarding the Sixth Instance, the SPT Terminal Servers reside within a PSP and an ESP, thus restricting access to only authorized personnel.

URE's Mitigation Plan (RFCMIT011281) is discussed with violations RFC2014014066, RFC2014014067, and RFC2014014068 above.

<u>CIP-007-3a R6.1, R6.4 (RFC2014014063, RFC2014014064, RFC2014014065)</u>

ReliabilityFirst determined that URE failed to produce evidence that logs of system events relating to cyber security were maintained and reviewed for a minimum of 90 days. The violation affected devices owned by the corporate security, IT services, and transmission systems management functional groups. These groups could not provide evidence regarding what logs were reviewed, how they were reviewed, or when the reviews were completed. The failure was due to the fact there were multiple logging mechanisms across the organization that led to inconsistent processes.

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

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. Specifically, for the sample that ReliabilityFirst reviewed, URE could not provide evidence for almost half of the devices regarding which logs they were reviewing, how they were reviewing the logs, or when they completed the reviews. System event logs related to Cyber Assets are important to detect and prevent any security incidents. Lack of an adequate logging mechanism and periodic review of relevant logs significantly weakens URE's position to detect, investigate, and resolve security events

URE's Mitigation Plan (RFCMIT011261) to address these violations, and the violations of RFC2014013324, RFC2014013330, RFC2014013338 discussed below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. file necessary TFEs for affected SPT systems that require a TFE;
2. review logging capabilities for the current logging tools and CIP environment to determine a master tool or set of tools that can be used to collect Cyber Asset logs with the goals of reducing the number of logging tools to a minimum. URE will ensure that the master logging and analysis system has capabilities for automated log analysis and alert triggers that are customizable to meet URE and CIP security requirements;

3. determine the requirements to establish the URE cyber security operation center as the single source for log collection and analysis;
4. review current URE processes used for log collection and analysis to determine which meet the CIP security Standard requirements and can be used in the creation of a methodology and processes to be used by the URE cyber security operation center or the four departments if the URE cyber security operation center cannot be setup as the central logging and analysis center;
5. conduct interviews with logging and log analysis SMEs to determine possible improvements in process execution for the different processes to assist in arriving at a single set of corporate-wide processes;
6. determine log review and automated alerting criteria to cover the requirements for CIP Version 3 and Version 5;
7. generate recommendation on corporate-wide master logging and analysis tool set for review and approval using the results of the logging tool review, process review, SME interviews, and logging and analysis criteria;
8. generate process documentation based on the process reviews, SME interviews, development of manual and automated analysis criteria, and handling of potential security events;
9. implement the methodology of logging and standardized tool set;
10. train all URE personnel on the appropriate logging methods and tools used by each group and cyber security operation center staff to handle collected log data; and
11. review log collection an analysis after deployment to verify correct execution and additional areas of improvement.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R6.5 (RFC2014013324, RFC2014013330, RFC2014013338)

ReliabilityFirst determined that URE failed to implement and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. The violation included incomplete workforms for log reviews and SPT terminal servers placed into service without the capability of generating logs.

ReliabilityFirst determined the duration of the violations to be from the date URE needed to comply with the Standard, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The security event logs for the Cyber Assets in question were reviewed in a timely and consistent manner—only the workform was not completed. The SPT terminal servers do not have external communication capabilities since they were configured to only communicate within the ESP, thereby reducing the possibility of a compromise.

URE's Mitigation Plan (RFCMIT011261) is discussed in violations RFC2014014063, RFC2014014064, and RFC2014014065 above.

CIP-007-3 R8.2, R8.3 (RFC2014014060, RFC2014014061, RFC2014014062)

ReliabilityFirst determined that URE failed to execute its CVA to verify that only ports and services required for operation were enabled nor did it review controls for default accounts for Energy Management Systems (EMS) and PACS. While URE was able to demonstrate some reviews of ports and service and default accounts, it was not able to do so for all Cyber Assets. URE lacked effective asset and configuration management and verification controls, had incomplete processes, and inadequately trained personnel.

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

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. Specifically, not reviewing enabled ports and services can create unidentified vulnerabilities into the network by creating possible access points into the network, which increases risk of unauthorized access to critical systems. In addition, a review of default accounts to verify they have been disabled or renamed and the password changed is critical to protecting Cyber Assets. Finally, not reviewing default accounts potentially allows external personnel with knowledge of default credentials to gain access to critical systems.

URE's Mitigation Plan (RFCMIT011260) to address these violations, and the violations RFC2014013325, RFC2014013331, and RFC2014013339 below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. update baseline documentation to include "listening" ports as well as "established" ports and services information;

2. review and update URE policies and processes on what is required for documentation of ports and services information for all Cyber Assets and require all URE departments to use the same policies and procedures for recording ports and services information;
3. review and update policies and process on what is required for default, root, administrative, and other special account controls and require all URE departments to use the same policies and procedures for recording account information;
4. determine method for collection and documentation of all ports and services required for normal operation (i.e. baseline);
5. execute training for all URE personnel responsible for CIP environment ports and services and default, root, administrative, and other special accounts on the required information and maintenance of the information;
6. review and update the URE CVA process for gaps in information required and require all URE departments to use the same process for review of default, root, administrative, and other special accounts. URE would develop internal controls to trap for collection errors and comparison errors and streamline the collection of the required data and will consider and emphasize automated methods;
7. execute the updated CVA process, which will include a review all CVA baseline data and verification that data reflects the current operational conditions; and
8. correct the baseline data for instances discovered during the CVA activities where the baseline data did not reflect current operational conditions.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R8.3, R8.4 (RFC2014013325, RFC2014013331, RFC2014013339)

ReliabilityFirst determined that URE failed to include evidence of a review of controls for default accounts in its CVA documentation. The violation related to Cyber Assets owned by URE departments for engineering and asset management, corporate security, and IT services.

ReliabilityFirst determined the duration of the violations to be from the date of URE’s CVA, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. Specifically, a review of default accounts to verify they have been disabled or renamed and the password changed is critical to protecting Cyber Assets. Not reviewing default accounts potentially allows external personnel with knowledge of default credentials to potentially gain access of critical systems.

URE's Mitigation Plan (RFCMIT011260) is described in RFC2014014060, RFC2014014061, and RFC2014014062 above.

CIP-008-3 R1.6 (RFC2014014075, RFC2014014076, RFC2014014077)

ReliabilityFirst determined that URE failed to complete several sections of its Cyber Security Incident Response Plan checklist or incorporate lessons learned from an actual cyber security incident into its Response Plan

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE updated its Response Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because the Cyber Security Incident Response Plan needs to be completely tested to adjust the Response Plan as necessary based on the test so that it can ensure its Response Plan will be effective in case of a security incident. However, the Response Plan otherwise met the CIP-008-3 requirements, and URE at least attempted to perform an annual test of the Response Plan, thus reducing the risk that the plan will be ineffective in case of an actual security incident.

URE's Mitigation Plan (RFCMIT011259) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. conduct a table-top exercise observers in attendance with a goal of acquiring a different perspective and input for the lessons learned;
2. hold a follow-up meeting to review and discuss lessons learned with all participants and observers;
3. prepare a lessons learned final report describing the ideas and outcome of the exercise, and the discussions during the lessons learned meeting;
4. update the Response Plan to incorporate the exercise results and lessons learned from the final report;

5. add clarifying instructions to the response checklist that are consistent;
6. supplement the Response Plan with a matrix for systems and required responses;
7. establish role-specific evidentiary records by creating a tracking system for recording actions performed by each URE group during execution of the Response Plan;
8. develop a role specific training course for the cyber security incident response team participants; and
9. conduct a role-specific training course for the cyber security incident response team participants.

URE certified that the above Mitigation Plan requirements were completed.

CIP-009-3 R5 (RFC2014013378, RFC2014013379)

ReliabilityFirst determined that URE failed to test information on backup media that is essential to recovery annually. The violation involved multiple Cyber Asset classes at multiple locations—the information was not available in the location specified as required by the Recovery Plan.

ReliabilityFirst determined the duration of the violations to be from when URE updated its Recovery Plan but failed to validate that the recovery information was available at the location identified for certain CCAs, through when URE validated the missing information.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the BPS. Specifically, in order to accomplish the restoration of functionality of a CCA, URE need to obtain the essential information to recover the asset and reestablish the functionality previously served by the failed asset. If URE would lose a CCA at one of these locations, they could rebuild it from scratch, but if the information to recover the asset is not identified and available, it will hinder timely recovery of that Cyber Asset. Depending on the CCA and the function it performs, this may cause serious harm to a critical location, and in turn the BPS.

The risk was partially mitigated because URE could restore the CCA functionality by replacing the failed Cyber Assets. As an example, a relay, for which the function is protecting a transmission line, has an alarm indicative of a malfunction. The URE would investigate that alarm with onsite recovery practices described as part of their recovery plans. In addition, to ensure reliability of the BPS, URE follow operational procedures to replace the Cyber Asset with an equivalent device. They execute this by following the change and configuration management practices required by the CIP Standards.

The URE Mitigation Plan (RFCMIT010801 and RFCMIT010801) to address these violations were submitted to ReliabilityFirst.

The URE Mitigation Plan required URE to:

1. conduct a root cause analysis;
2. validate availability for the missing Cyber Asset recovery information; and
3. conduct a comprehensive review of recovery information for all Cyber Assets.

URE certified that the above Mitigation Plan requirements were completed.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of four hundred twenty-five thousand dollars (425,000) for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors, additional detail on each of the below factors is included in the Settlement Agreement:

1. URE has a compliance history that includes instances of noncompliance with NERC Reliability Standards. ReliabilityFirst considered these prior violations as aggravating factors in the penalty determination;
2. URE has completed all mitigating actions for all violations, and as a result, ReliabilityFirst has determined that URE is appropriately managing, monitoring, and mitigating the risk posed by the violations;
3. although URE's issues that are more significant were mostly centralized in specific areas, URE went above and beyond the actions required to mitigate the violations and committed to overhaul the entire CIP Compliance Program in order to better coordinate and streamline processes and enhance overall security posture. ReliabilityFirst awarded mitigating credit for these measures;
4. ReliabilityFirst will perform a Spot Check of URE. This Spot Check will include two components. First, the Spot Check will include an evaluation of evidence related to implementation of the above and beyond action items. Second, the Spot Check will include a review of URE's current state of compliance for a targeted sample of the CIP Reliability Standard Requirements;
5. URE was cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

7. of the 70 discrete sets of facts and circumstances included in the violations, ReliabilityFirst determined that 24 posed a minimal risk, 28 posed a moderate risk, and the 18 remaining posed a serious and substantial risk to the reliability of the BPS;
8. URE completed several of the remediation activities described above before ReliabilityFirst conducted the Compliance Audit. ReliabilityFirst considered URE's response to the violations to be exemplary, so it awarded a significant amount of credit to encourage similar responses by URE and other registered entities in the future; 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 monetary penalty of four hundred twenty-five thousand dollars ($425,000) 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[6]

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,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on August 11, 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.

[6] *See* 18 C.F.R. § 39.7(d)(4).

[7] *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).

In reaching this determination, the NERC BOTCC considered the factors considered by ReliabilityFirst as listed above, as well as the following factors:

1. ReliabilityFirst worked collaboratively with URE to implement mitigation and above-and-beyond solutions that should help URE maintain secure and reliable operations for at least the next few years;
2. while ReliabilityFirst favored expenditures on such solutions over a higher monetary penalty, the $425,000 penalty is significant;
3. beyond the monetary penalty, the Spot Check will allow ReliabilityFirst to assure that URE is maintaining the improved systems and processes implanted during the mitigation process;
4. the Settlement Agreement balances the goals of deterring undesired conduct by registered entities and encouraging aggressive mitigation, above-and-beyond activities, and cooperation by registered entities; and
5. URE's conduct in completing all mitigating actions within nine months, maintaining constant communication and transparency with regional staff, contrasts with the conduct of entities receiving a larger assessed penalty with a similar number of violations.[8]

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of four hundred twenty-five thousand dollars ($425,000) 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.

[8] *See, e.g.*, NP14-48-000 covering 100 violations of CIP Standards for a total penalty of $625,000.

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net *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.	Sonia C. Mendonça* Deputy General Counsel, Vice President of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net 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

	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 Kristen M. Senk* Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-06769 216-503-9207 facsimile kristen.senk@rfirst.org

Conclusion

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

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

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

cc: Unidentified Registered Entity
ReliabilityFirst Corporation