May 31, 2018

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. NP18-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) 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]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] 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 22 violations of the Critical Infrastructure Protection (CIP) NERC Reliability Standards.

---

[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 (2018). *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.

According to the Settlement Agreement, URE admits to the violations and has agreed to the assessed penalty of one hundred eighty thousand dollars ($180,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between ReliabilityFirst and URE. The details of the findings and basis for the penalty are set forth 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 (2018), 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 herein.

Violation(s) Determined and Discovery Method *SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
RFC2015014936	CIP-003-3	R5	Lower/ Severe	SR	Minimal	$180K
RFC2016015692	CIP-003-3	R5	Lower/ Severe	SR	Moderate	
RFC2015015313	CIP-003-3	R6	Medium/ Severe	SR	Minimal	
RFC2016015717	CIP-003-3	R6	Lower/ Severe	SR	Minimal	
RFC2015015008	CIP-004-3a	R3	Medium/ Moderate	SR	Minimal	
RFC2015015009	CIP-004-3a	R4	Lower/ High	SR	Minimal	
RFC2015015402	CIP-004-3a	R4	Lower/ Severe	SR	Minimal	
RFC2016015716	CIP-004-3a	R4	Lower/ Severe	SR	Minimal	
RFC2016016474	CIP-005-3a	R1	Medium/ Severe	SR	Moderate	
RFC2015015314	CIP-006-3c	R1	Medium/ Severe	SR	Minimal	
RFC2016015844	CIP-006-3c	R5	Medium/ Severe	SR	Serious	
RFC2016015715	CIP-007-3a	R1	Medium/ Severe	SR	Minimal	
RFC2016015714	CIP-007-3a	R2	Medium/ Severe	SR	Moderate	

RFC2015015241	CIP-007-3a	R3	Lower/ Severe	SR	Minimal	
RFC2016015843	CIP-007-3a	R3	Lower/ Severe	SR	Minimal	
RFC2016015538	CIP-007-3a	R5	Lower/ Severe	SR	Minimal	
RFC2016015713	CIP-007-3a	R5	Medium/ Severe	SR	Moderate	
RFC2016015752	CIP-007-3a	R6	Medium/ Severe	SR	Moderate	$180K
RFC2015015107	CIP-007-3a	R6	Lower/ Severe	SR	Minimal	
RFC2017017565	CIP-007-6	R2	High/ Severe	CA	Minimal	
RFC2017017566	CIP-007-6	R5	Medium/ High	CA	Minimal	
RFC2015015312	CIP-014-2	R1	High/ Lower	SR	Moderate	

RISK COMMON TO THE VIOLATIONS

ReliabilityFirst determined the penalty in this case based on the six moderate risk violations and the one serious risk violation.

Fifteen of the violations posed a minimal risk, six posed a moderate risk, and one posed a serious and substantial risk to the reliability of the bulk power system (BPS). ReliabilityFirst determined the violations do not involve and are not indicative of programmatic issues across URE's CIP compliance program. URE implemented internal controls that identified many of the instant violations. While most of the violations were short in duration, or relatively short, several of the moderate risk violations had longer durations (up to two years), indicating a potential weakness in detective controls in these areas.

Nevertheless, these moderate risk violations generally involved isolated systems or assets, and thus, did not involve programmatic or systemic issues.

URE had some internal controls in place that mitigated the risk to the BPS. For example, URE's buildings and Physical Security Perimeters (PSPs) were under surveillance 24 hours a day, seven days a week; Physical Access Control Systems (PACSs) were isolated, requiring authorized physical and electronic access; Bulk Electric System (BES) Cyber Assets had both logical and physical protection; and URE used detective logging and alarming tools.

The serious risk violation provided the opportunity for undetected compromise of an unmanned, critical substation and showed URE's inability to respond due to lack of situational awareness. While the risk was somewhat mitigated because certain assets were being monitored via an alert and monitoring program, which would have detected unauthorized changes, and local physical access controls were working, URE's headquarters could not monitor or communicate with the site and thus would have been unaware of and unable to respond to an intrusion.

CIP-003-3 R5 (RFC2015014936) - OVERVIEW

ReliabilityFirst determined that URE failed to document and implement a program for managing access to protected Critical Cyber Assets (CCAs) as required by CIP-003-3 R5, in three separate instances. In two instances, employees did not immediately pick up printed versions of CIP documents from printers. In the third instance, URE inadvertently set the confidentiality classification level for a CIP process document to "public" view on its internal site.

ReliabilityFirst determined the duration of the violation to be approximately one year and nine months, from when the confidential document was inadvertently set to "public" view, to the date by which all three instances were mitigated by protecting or destroying the confidential information.

The violation involved the management practices of external interdependencies and workforce management. External interdependencies management was involved because URE's contractor failed to protect CIP information as required. Workforce management was involved because, in all three instances, additional training and awareness could have helped to prevent these errors.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Identify and implement a technological solution to control and monitor end-point printing;
2. Train on and validate the solution's effectiveness;
3. Identify changes required to maintain integrity of documents within the document repository when updating, changing, or moving documents;
4. Prevent URE resources from uploading documentation directly to internal site through a certain mode, therefore forcing documentation to be added in an approved and documented method; and
5. Validate the metadata prior to document publication.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-003-3 R5 (RFC2016015692) – OVERVIEW

ReliabilityFirst determined that URE failed to document and implement a program for managing access to protected CCAs as required by CIP-003-3 R5. Specifically, a URE reliability assurance team member was able to access a file in a URE NERC compliance information folder, which contained CIP protected information.

ReliabilityFirst determined the duration of the violation to be approximately two years and one month, from the date URE permitted unauthorized individuals access to CIP information, to the date URE completed its Mitigation Plan.

The violation involved the management practice of asset and configuration management because URE did not have an accurate understanding of the effects of the configurations of folders within its access system.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Investigate and resolve issues with folder permissions on the relevant folder;
2. Identify folders that contain information utilizing a certain document (URE's list of approved BES Cyber System information repositories) as well as existing enterprise job roles;
3. Contact CIP data owners to confirm that all of their repositories are listed on the relevant repository list document;
4. Create a procedure for how new file share repositories will be created on servers;
5. Create a procedure to migrate the folders identified in milestone two;

6. Migrate the relevant folders; and
7. Remove creator owner permissions from all shared folders identified in milestone two.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-003-3 R6 (RFC2015015313) – OVERVIEW

ReliabilityFirst determined that URE failed to have minimum security management controls in place to protect CCAs. Specifically, an analyst added a device to URE's logging tool, and added the correct group to receive the alerting for the device. The next day, another analyst deleted the device from the logging tool. Thereafter, the logging tool was retaining logs for a certain device, but the device was not in the correct group to alert on the required conditions.

ReliabilityFirst determined the duration of the violation to be approximately four-and-a-half months, from the date the device was deleted and thus not alerting, to the date URE added the device to the correct alerting group.

The root cause of this violation was that an analyst did not follow the proper change management process despite being trained on the proper procedure for change management. This violation involved the management practices of asset and configuration management and workforce management. Asset and configuration management was involved because URE did not adhere to its configuration management process. Workforce management was involved because URE staff did not adhere to their internal procedures and controls in configuring a Cyber Asset.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Terminate the analyst as a result of not satisfactorily performing his job responsibilities relating to this incident and other actions;
2. Determine the extent of condition by verifying that all assets which are defined in URE's CCA lists are sending logs to the logging tool and are associated with the correct groups to generate alerts defined in a relevant security status monitoring process;
3. Evaluate the solution to monitor the configuration of the logging tool's log sources that controls CIP alerting and test email alerting;

4. Build a new rule in the logging tool to alert the manager of the cyber security department and the director of networks and information security department after the logging tool has not received logs from a certain period of time;
5. Implement a solution to monitor the logging tool's log source group defined that controls CIP alerting and configured email alerts to the cyber security team when there are changes to that group;
6. Update the processes and work forms associated with change management and commissioning to include specific controls an asset administrator must act upon to ensure CIP-005 and CIP-007 controls are addressed in alignment with the current CIP version; and
7. Conduct a page-turn training session of newly proposed processes and work forms, and address all applicable questions and concerns during the page-turn exercise.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-003-3 R6 (RFC2016015717) – OVERVIEW

ReliabilityFirst determined that URE failed to have minimum security management controls in place to protect CCAs. Specifically, in two instances URE did not follow the established change management process: first, when URE deployed a PACS intelligent controller into production, and second, when URE made changes to several assets.

ReliabilityFirst determined the duration of the violation to be approximately 10 months, from the date URE was required to comply with CIP-003-3 R6, to the date URE completed its Mitigation Plan.

Regarding the first instance, the root cause was lack of managerial oversight during a transition process where URE was transitioning the responsibility of the PACS devices from its security department, which did not have the appropriate technical expertise, to its engineering group. This violation occurred during the transition time when these Cyber Assets were being incorporated into the engineering group's change control process. Regarding the second instance, the violation involved the management practices of asset and configuration management and workforce management. Asset and configuration management was involved because URE did not adhere to its configuration management process. Workforce management was involved because URE staff did not adhere to their internal procedures and controls in configuring a Cyber Asset.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Complete changes to the engineering change control process to align with CIP Version 5;
2. Update engineering CIP Cyber Asset management system (CAMS) to align with the new change control process;
3. Develop CIP Version 5 capable baseline configuration in CAMS;
4. File and obtain approval of Technical Feasibility Exceptions (TFEs) for the PACS to complete CIP Version 5 commissioning tasks in CAMS;
5. Develop a separate security configuration procedure for the relevant controller;
6. Complete commissioning and change control tasks for assets installed at the relevant locations;
7. Establish a change review board;
8. Train all engineering personnel responsible for the use of CAMS for all CIP changes on related systems;
9. Implement a new change management tool; and
10. Train relevant teams on the use of the new change management tool.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-004-3a R3 (RFC2015015008) – OVERVIEW

ReliabilityFirst determined that URE failed to have a documented Personnel Risk Assessment (PRA) program for personnel having authorized cyber or authorized unescorted physical access to CCAs. Specifically, URE granted four employees unescorted physical access without appropriately documented PRAs.

ReliabilityFirst determined the duration of the violation to be approximately one month, from the date URE granted unescorted physical access without the requisite PRAs, to the date URE revoked the access.

Regarding the root cause, a specialist reviewed a large number of identities over a three-day period during the rollout of URE's new role-based access process, which led to these four errors in the process. This violation involved the management practice of work management and verification as the errors were caused because of having to review many PRAs in a short period, and not conducting a review to verify that there were no errors in that review process.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Conduct individual counseling with the security specialist;
2. Conduct a meeting with the impacted groups to discuss the incident;
3. Conduct reinforcement training of all corporate security personnel involved with CIP-004-3 R3 compliance;
4. Formulate a likelihood risk-based PRA review methodology;
5. Conduct a review of PRA documentation for those identified individuals and took immediate action on any issues identified therein; and
6. Revise URE policy requiring URE corporate security to perform PRAs on all individuals requiring any level of unescorted access, whether CIP or non-CIP in nature, thus eliminating the reliance on another entity to perform the PRA.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-004-3a R4 (RFC2015015009) – OVERVIEW

ReliabilityFirst determined that URE failed to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs. Specifically, this violation involves three instances of URE not properly revoking access within the seven-day period.

ReliabilityFirst determined the duration of the violation to be approximately one year, from the date URE was required to comply with CIP-004-3a R4, to the date URE completed its Mitigation Plan.

The violation involved the management practice of workforce management because they involve employees taking some, but not all steps necessary to complete revocation in a timely manner as a result of rushing through the tasks. Additionally, URE could have had additional controls in place to ensure the employees completed all necessary steps to revoke access in a timely manner.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Modify the workflows for all access revocation-related requests to include a reviewer step;
2. Identify any additional identities with “invalid” termination dates;
3. Disable future termination capability;
4. Train system administrators of the identity access system regarding the capability changes and process handling;

5. Modify workflows to accommodate an escalation process for all individual access revocations; and
6. Review and revise the process and requirements for revocation of access when a temporary leave of absence occurs.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-004-3a R4 (RFC2015015402) – OVERVIEW

ReliabilityFirst determined that URE failed to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs. Specifically, access for one URE employee located at another registered entity's facility was not properly revoked within the seven-day period.

ReliabilityFirst determined the duration of the violation to be approximately four-and-a-half months, from the date URE was required to remove the employee's access to the date URE removed the access.

The root cause was that the registered entity that owned the facility the employee was located failed to follow the procedure for notifying URE when an employee no longer needs access. Additionally, URE's additional proactive measure, where URE sent weekly emails to the registered entity identifying the individuals who currently had access, failed because the registered entity did not properly review the weekly email. URE had been sending the registered entity the weekly emails since before the violation began. The email should have prompted the registered entity to inform URE of the individual's departure from the company within the required timeframe. The violation also involved the management practice of external interdependencies because URE failed to mitigate risks relating to third parties

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Request access removal form from the registered entity;
2. Receive access removal form;
3. Request follow-up resignation data regarding the employee in question;
4. Receive resignation data from the registered entity;
5. Receive results of the registered entity's internal investigation;
6. Set up a meeting with the registered entity to identify corrective or preventive actions;

7. Reinforce with the registered entity the CIP-004-3 and future CIP-004-5 access removal requirements;
8. Receive evidence of the registered entity's internal training regarding CIP-004 access removal requirements; and
9. Revise the unescorted physical access agreement between URE and the registered entity.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-004-3a R4 (RFC2016015716) – OVERVIEW

ReliabilityFirst determined that URE failed to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs. Specifically, access for one URE employee was not properly revoked within the seven-day period after changing job duties within URE.

ReliabilityFirst determined the duration of the violation to be approximately two weeks, from the date URE should have removed access, to the date URE removed access.

The root cause was an unclear designation of CIP versus non-CIP access within URE's alert tool, which contributed to human performance issues in completing the access removal tasks. This violation involved the management practice of workforce management because additional training, along with clearer designations in the system, could have helped prevent this violation.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Introduce and train affected personnel on the new CIP Standards;
2. Launch a new CIP access revocation process; and
3. Email notifications from the alert tool with priority status to revoke CIP access initiated.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-005-3a R1 (RFC2016016474) – OVERVIEW

ReliabilityFirst determined that URE failed to ensure that every CCA resided within an Electronic Security Perimeter (ESP). Specifically, URE did not identify and document an access point to the ESP.

ReliabilityFirst determined the duration of the violation to be approximately one year and seven months, from the first date that a substation technician was dispatched to perform maintenance that required connection to both CAMs and a BES Cyber Asset, to the date URE completed its Mitigation Plan.

The violation involved the management practice of verification because URE failed to verify that it properly identified and understood all external routable connections and access points.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Update URE's cyber security policy to address that URE resources shall only utilize URE authorized Transient Cyber Assets (TCAs) when connecting to a High or Medium impact BES Cyber System(s), Protected Cyber Asset(s), and/or ESP(s);
2. Implement a project plan for TCAs that will include technical, procedural, and process controls to prevent TCA laptops from becoming unintended access points;
3. Drafted, as part of the project plan, a test plan which establishes technical controls that disable a TCA laptop's logical input and output ports (Ethernet and console ports) when connected to URE's Virtual Private Network (VPN);
4. Execute, as part of the project plan, the technical controls test plan and provide evidence showing the results that the TCA laptop's logical input and output ports are disabled when connected to URE's VPN.
5. Perform, as part of the project plan, training with URE resources in the field on how to use the technical and cyber security controls on a TCA laptop; and
6. Deploy, as part of the project plan, TCA laptops to authorized TCA users.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-006-3c R1 (RFC2015015314) – OVERVIEW

ReliabilityFirst determined that URE failed to document, implement, and maintain a physical security plan as required by CIP-006-3c R1. Specifically, during a routine inspection URE discovered that an air conditioning unit was an exploitable access point into an identified PSP.

ReliabilityFirst determined the duration of the violation to be approximately 11 months, from the date URE was required to comply with CIP-006-3c R1.1, to the date URE completed its Mitigation Plan.

The root cause was a lack of communication prior to installing the air conditioning unit. This violation involved the management practice of grid maintenance because URE failed to maintain properly its facilities.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Review the violation with the facilities manager to clearly identify the issue and impacts;
2. Seal and secure the access point to the PSP;
3. Conduct a lessons learned meeting to review the violation and the root cause with the supply chain and facilities group;
4. Create and publish a new process document; and
5. Conduct training of all affected groups on the process document.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-006-3c R5 (RFC2016015844) – OVERVIEW

ReliabilityFirst determined that URE failed to document and implement the technical and procedural controls for monitoring physical access at all access points to the PSPs 24 hours a day, seven days a week. Specifically, the power supply to a security rack was shut off during maintenance work at one of URE's facilities, and for six days afterwards the facility was not communicating with URE's headquarters.

ReliabilityFirst determined the duration of the violation to be approximately six days, from the date URE failed to monitor physical access, to the date URE restored monitoring capabilities.

The violation involved the management practices of grid maintenance and workforce management. Grid maintenance was involved because URE did not properly mitigate the risks of the maintenance work on the station. More specifically, URE's vendor properly submitted a maintenance ticket, but there was a miscommunication between groups, so URE and the vendor did not consider the security systems that operate on the same network where the maintenance activities were being performed.

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

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Complete repairs and re-establish security monitoring at the relevant facility;
2. Conduct PACS incident lessons learned meeting;
3. Revise security command center alarm response policy to clarify responsibilities;
4. Review current processes and practices to determine a need for alignment with roles and responsibilities;
5. Revise or create documentation regarding roles and responsibilities;
6. Provide training on new or revised policies and processes regarding PACS outage reporting, troubleshooting, and communications;
7. Develop PACS service level agreement policy document that documents responsibilities for the use, maintenance, and management of physical security controls; and
8. Approve and implement PACS service level agreement.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R1 (RFC2016015715) – OVERVIEW

ReliabilityFirst determined that URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls. Specifically, a URE asset administrator performed a PACS modification, but did not complete the change and configuration management process documentation for a device that was replaced.

ReliabilityFirst determined the duration of the violation to be approximately seven months, from the date URE introduced the assets into its environment, to the date by which URE completed the change control activities.

The root cause was a lack of workforce management in that the corporate security department charged with managing the assets did not have expertise to provide technical oversight of the PACS devices.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Complete changes to engineering change control process to align with CIP Version 5;

2. Update the engineering CIP CAMS to align with the new change control process;
3. Develop CIP Version 5 baseline configuration in the engineering CAMS.
4. File and obtain approval of TFEs for the PACS to complete CIP Version 5 commissioning tasks in CAMS;
5. Develop and implement a separate security configuration procedure for relevant controllers;
6. Complete commissioning and change control tasks for assets installed at the relevant locations; and
7. Train all engineering personnel responsible for the use of CAMS for all CIP changes on related systems.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R2 (RFC2016015714) – OVERVIEW

ReliabilityFirst determined that URE failed to establish, document, and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled. Specifically, URE had multiple undocumented services with ports enabled related to its PACS, and one of those ports was unnecessary for operations.

ReliabilityFirst determined the duration of the violation to be approximately eight months, from the date URE was required to comply with CIP-007-3a R2, to the date URE completed its Mitigation Plan.

The violation involved the management practices of verification and workforce management. Verification management was involved because URE failed to verify and document that the ports and services were necessary for operations.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Reassign these Cyber Assets to an asset manager capable of reviewing CIP controls;
2. Implement a new monitoring program; and
3. Verify its Cyber Vulnerability Assessment (CVA) Action Plan to remove the undocumented ports and accounts.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-6 R2 (RFC2017017565) – OVERVIEW

ReliabilityFirst determined that URE failed to implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-6 Table R2-Security Patch Management. Specifically, URE was two weeks late in completing evaluations of security patches for two Cyber Assets, which were both PACS.

ReliabilityFirst determined the duration of the violation to be approximately two weeks, from the date by which URE was required to complete the evaluations, to the date URE completed the evaluations.

The root cause was an error in calculating the date to perform the evaluation of security patches. The calculation for the next security patch evaluation was based on the implementation of the previous month's security patches rather than the previous evaluations.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Conduct a meeting to discuss patch evaluation process changes with asset managers;
2. Draft proposed document changes and distribute them for comments;
3. Hold a meeting to review and finalize changes to process documents with asset managers;
4. Publish updated documents to URE's internal site; and
5. Determine if automatic notifications can be implemented based on available technology and resources.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R3 (RFC2015015241) – OVERVIEW

ReliabilityFirst determined that URE failed to establish, document, and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP. Specifically, URE failed to install three sets of patches in a timely manner, and no compensating measures were documented to mitigate risk exposure.

ReliabilityFirst determined the duration of the violation to be approximately three-and-a-half months, from the date by which URE was required to implement the first set of patches, to the date URE evaluated the third set of patches.

The root cause is that there were too many individuals involved in the patching process and roles and responsibilities were not clear. Additionally, this violation involved the management practice of asset and configuration management because URE's processes lacked sufficient controls to manage the timely implementation of changes to assets.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Facilitate CIP server patching transition meetings;
2. Have the engineering department walk through the current process with the server team;
3. Take an inventory and review CIP forms by asset type/class that are completed by the engineering and security departments for CIP patching with the server team;
4. Implement a relevant patching tool and integrate it to all applicable CIP Cyber Assets;
5. Provide the server team with asset baseline information and historical patching data;
6. Have the engineering department provide a review of the previous patch evaluation performed by the server team;
7. Transition the operating system patch management duties for certain servers to the server team;
8. Update process documents to reflect common process across the multiple asset classes the server team will be handling in the future;
9. Perform an extent of condition assessment to identify any missing patches on the Cyber Assets; and
10. Remediate all missing patches on all applicable CIP Cyber Assets following the change management process.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R3 (RFC2016015843) – OVERVIEW

ReliabilityFirst determined that URE failed to establish, document, and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP. Specifically, URE failed to patch a certain server and failed to evaluate software supplied and installed by URE on associated devices.

ReliabilityFirst determined the duration of the violation to be approximately one year and eight months, from the date the asset was declared a PACS, to the date URE completed its Mitigation Plan.

The root cause was miscommunication between URE and its vendor. The vendor agreement stated that the vendor would assist in the evaluation and implementation of patches. The violation involved the management practices of external interdependencies and workforce management. External interdependencies management was involved because URE's coordination with the external vendor did not assure that patches were installed in a timely fashion. Workforce management was involved because URE staff did not properly secure or control the PACS logging system.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Patch the relevant server;
2. Update procedures to include the relevant server in the server teams' procedure;
3. Incorporate the relevant server into the server team's monthly patching process;
4. Perform an extent of condition assessment to find and address any other CIP assets that have any patching deficiencies; and
5. Remedy any patching deficiencies found during the extent of condition assessment.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R5 (RFC2016015538) – OVERVIEW

ReliabilityFirst determined that URE failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. Specifically, URE did not change one password for a relay despite documentation stating the password was changed.

ReliabilityFirst determined the duration of the violation to be approximately three months, from 15 months from the prior password change, to the date URE changed the password.

This violation involved the management practice of verification, as URE did not have a verification process to ensure that all passwords were changed.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Update the relevant driver to support a relevant relay model, which allows for the automatic update of passwords to occur annually;
2. Revise the relevant baseline testing and approval of engineering Cyber Assets process to include a step/instruction to update the relevant drivers if applicable; and
3. Train employees and contractors during a safety stand down.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R5 (RFC2016015713) – OVERVIEW

ReliabilityFirst determined that URE failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. Specifically, URE had three relevant instances wherein user accounts were either not documented, had insufficient administrator rights, or lacked approved access records.

ReliabilityFirst determined the duration of the violation to be approximately one year and seven months, from the date URE was required to comply with CIP-007-3a R5, to the date URE completed its Mitigation Plan.

The violation involved the management practices of external interdependencies and workforce management. External interdependencies management was involved because URE's access provision for its external vendor did not provide the necessary approval. Workforce management was involved because URE staff did follow procedures to document user accounts properly.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Reassign the relevant Cyber Assets to an asset manager capable of reviewing CIP controls;
2. Implement a new baseline monitoring program;
3. Verify that its CVA Action Plan to remove the undocumented accounts was implemented;
4. Establish a team and conduct a series of meetings to develop a service level agreement between departments;
5. Use the service level agreement forum to determine the required permissions for each functional group;
6. Implement the appropriate access between each functional group;

7. Include relevant security shared accounts in an URE centralized password safe;
8. Create relevant security roles in the access request system to document who has access to the password safe; and
9. Create requests and grant access through the access request system for individuals needing access to the relevant security system.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-6 R5 (RFC2017017566) – OVERVIEW

ReliabilityFirst determined that URE failed to implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-6 Table R5-System Access Controls. Specifically, URE failed to change passwords at least once every 15 calendar months for a shared account that could be used for interactive user access for two Cyber Assets, both PACS.

ReliabilityFirst determined the duration of the violation to be approximately two-and-a-half months, from the date by which URE should have changed the passwords, to the date by which URE changed the passwords.

The root cause was an error during transition when the servers came under the ownership of the server team. The violation involved the management practice of verification because URE failed to verify that each PACS had current patches after the transition to the server team.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Change the password for the relevant account in the related database program;
2. Discuss with groups to see if changes to process and documentation is required;
3. Establish extent of condition;
4. Update and publish any required document revisions;
5. Validate all asset password last-changed dates are synced with the relevant database program; and
6. Create a checklist for adding a new account in the relevant database program and validating the last change.

URE certified that all mitigation actions were completed.

CIP-007-3a R6 (RFC2015015107) – OVERVIEW

ReliabilityFirst determined that URE failed to ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security. Specifically, when URE commissioned four devices they inadvertently created firewall rules that disallowed logging.

ReliabilityFirst determined the duration of the violation to be approximately one month, from the date URE commissioned the devices, to the date the devices began sending logs to the logging tool.

The issue occurred because of a hierarchy issue where a different device was programed incorrectly and placed higher in the hierarchy, thereby blocking traffic from the four devices. The violation involved the management practices of asset and configuration management and verification. Asset and configuration management was involved because URE failed to manage changes to the devices during the commissioning process. Additionally, verification was involved because URE failed to verify that the firewall rule correction worked as intended prior to commissioning the devices.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Terminate the cyber security analyst as a result of not satisfactorily performing his job responsibilities;
2. Determine the extent of condition by verifying that all assets which are defined in CCA lists are sending logs to the logging tool and are associated with the correct groups to generate alerts defined in its related process;
3. Evaluate a solution to monitor the configuration of the logging tool's log sources that controls CIP alerting and test email alerting;
4. Build a new rule in the logging tool to alert the manager of the cyber security department and the director of the networks and information security department after the logging tool has not received logs from a device in 96 hours;
5. Implement a solution to monitor the logging tool's logs;
6. Update the processes and work forms associated with change management and commission to include specific controls an asset administrator must act upon to ensure CIP-005 and CIP-007 controls are addressed in alignment with CIP Version 5;
7. Conduct a training session on newly proposed processes and work forms, and address all applicable Subject Matter Expert (SME) questions and concerns during the page-turn exercise;

8. Correct any findings or deficiencies discovered during the extent of condition analysis conducted in Milestone 2; and
9. Complete a CIP-007 R6 Mitigation Plan closure report.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R6 (RFC2016015752) – OVERVIEW

ReliabilityFirst determined that URE failed to ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security. Specifically, in two instances certain programs were not sending failed login attempt notifications to URE's logging tool.

ReliabilityFirst determined the duration of the violation to be approximately six months, from the date URE failed to monitor logs in the second instance, to the date URE completed its Mitigation Plan.

The violation involved the management practices of asset and configuration management because URE did not adhere to its configuration management process.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Investigate and resolve logging issues with the two relevant programs;
2. Establish a change review board;
3. Implement a certain monitoring program as a change management tool;
4. Train teams on change control process and the new monitoring program;
5. Update relevant documents for asset classes to include specific and proper logging configuration and specific testing measures to prove logging is functional;
6. Perform logging extent of condition assessment to analyze all CIP devices to ensure they are logging to the logging tool properly; and
7. Update any additional relevant documents to include specific and proper logging configuration and specific testing measures to prove logging is functional.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-014-2 R1 (RFC2015015312) – OVERVIEW

ReliabilityFirst determined that URE failed to perform an initial risk assessment and subsequent risk assessments of its transmission stations and transmission substations that meet the criteria specified in CIP-014-2. Specifically, URE did not assess one substation pursuant to Section 4.1.1 of the CIP-014-2.

ReliabilityFirst determined the duration of the violation to be approximately five days, from the date URE was required to comply with CIP-014-2 R1, to the date URE completed its risk assessment for the substation at issue.

The major contributing cause was a change to the baseline list of substations used during the evaluation process occurred (to add the substation) and was not communicated to those conducting the assessment. The violation involved the management practice of verification because URE failed to verify that each qualifying substation would be reviewed in compliance with CIP-014.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Perform a review of applicability Section 4.1.1 and identify all missing substations;
2. Perform risk assessments for missing substations;
3. Include a planning SME as a reviewer of CIP-002-5 BES Cyber Asset identification process results; and
4. Revise the CIP-014 R1 planning process to include a secondary review of the list of applicable substations to confirm it is complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of one hundred eighty thousand dollars ($180,000) for the referenced violations.

In reaching this determination, ReliabilityFirst considered the following factors:

1. URE had relevant prior violations of CIP-007-3a R2 and R5;
2. URE had an internal compliance program at the time of the violation, which was considered a mitigating factor in penalty determination;
3. URE self-reported 20 of the violations;

4. URE was highly cooperative throughout the compliance enforcement process;
5. there was neither evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. fifteen of the violations posed a minimal risk, six of the violations posed a moderate risk, and one violation posed a serious and substantial risk to the reliability of the BPS; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of one hundred eighty thousand dollars ($180,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

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

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the violations on May 8, 2018 and approved the terms of the Settlement Agreement. In approving the terms of the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the terms of the Settlement Agreement and believes that the assessed penalty of one hundred eighty thousand dollars ($180,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[4] *See* 18 C.F.R. § 39.7(d)(4).

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

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.

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

Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 jason.blake@rfirst.org (216) 503-0683 (216) 503-9207 facsimile Kristen M. Senk* Managing Enforcement Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 kristen.senk@rfirst.org (216) 503-06769 (216) 503-9207 – facsimile *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* Vice President, Deputy General Counsel, and Director 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 Director of Enforcement Oversight 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 Goldfin* Associate Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile robert.goldfin@nerc.net

Conclusion

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

Respectfully submitted,

/s/ Robert P. Goldfin

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
Robert P. Goldfin
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
robert.goldfin@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation