PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

January 30, 2014

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. NP14-29-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, 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 Reliability*First* Corporation (Reliability*First*) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from Reliability*First*'s determination and findings of the violations[3] of CIP-005-1, CIP-005-3a, CIP-005-3, CIP-006-1, CIP-007-1, and CIP-007-3. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of seventy-five thousand dollars ($75,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers RFC2013011941, RFC2013012708, RFC2012011452, RFC2012011455, RFC2012011568,

[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 (2013). *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).

[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.

RFC2012011569, RFC2013012114, RFC2013011942, RFC2013011943, RFC2013011945, RFC2012011453, RFC2012011454, and RFC2013013118 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, by and between Reliability*First* and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the 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 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Reliability*First* Corporation	Unidentified Registered Entity	NOC-2261	RFC2013011941	CIP-005-1	R2; R2.2	Medium	$75,000
			RFC2013012708	CIP-005-3a	R3; R3.2	Medium	
			RFC2012011452	CIP-005-3	R4	Medium	
			RFC2012011455	CIP-007-3	R8	Lower	
			RFC2012011568	CIP-006-1	R1	Medium	
			RFC2012011569	CIP-006-1	R2; R2.2	Medium	
			RFC2013012114	CIP-007-1	R1; R1.1	Medium	
			RFC2013011942	CIP-007-1	R2	Medium	
			RFC2013011943	CIP-007-1	R3	Lower	

			RFC2013011945	CIP-007-1	R4; R4.2	Medium	
			RFC2012011453	CIP-007-1	R5; R5.2	Lower	
			RFC2012011454	CIP-007-1	R6; R6.3, R6.4, R6.5	Medium	
			RFC2013013118	CIP-007-1	R6; R6.3, R6.4, R6.5	Medium	

CIP-005-1 R2; R2.2 (RFC2013011941)

The purpose statement of Reliability Standard CIP-005-1 provides in pertinent part: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-005-1 R2 provides in pertinent part:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> ***
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
>
> ***

CIP-005-1 R2 has a "Medium" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-005-1 R2. During a Compliance Audit, Reliability*First* discovered an additional instance of a violation of CIP-005-1 R2.

During URE's cyber vulnerability assessment (CVA), it performs a detailed ports and services assessment to ensure that only those ports and services necessary for secure operation are enabled. The resulting annual CVA then becomes the new baseline for ports and services. URE did not maintain this baseline configuration between annual CVAs. Instead, it restarted the baseline each year, meaning ports and services could have been modified without authorization since the last CVA without detection.

URE's document listing the ports and services does not document or tie the ports and services to individual assets or specified groupings to identify which ports and services should be enabled on which devices or device types. For at least one switch, certain ports were enabled but not listed as such in URE's document. In addition, there were three ports and services that were enabled that were not required for normal or emergency operations.

Reliability*First* determined that URE had a violation of CIP-005-1 R2 because it failed to enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter (ESP).

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to protect Electronic Security Perimeter (ESP) access points increases the likelihood of a gap in security defenses for the ESP. In addition, the lengthy duration of the violation increased URE's exposure to this risk. The risk to the reliability of the BPS was mitigated by the following factors. Although URE did not maintain a baseline between CVAs, each change to ports and services required prior approval through the change control process. In addition, the annual CVA change ticket assessments and the ports and services true-ups have not identified any unauthorized enabled ports and services. Regarding the issue, the devices at issue are located within an ESP and a Physical Security Perimeter (PSP). This means additional credentials are required to gain access to the devices, the site has restricted physical access, and the site is manned at all times. In addition, URE review of the open ports and services demonstrated that all but three of its open ports and services were required.

CIP-005-3a R3; R3.2 (RFC2013012708)

The purpose statement of Reliability Standard CIP-005-3a R3 provides: "Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-005-3a R3 provides in pertinent part:

> R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.
>
> ***
>
> R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

CIP-005-3a R3 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-005-3a R3. During a daily review, URE discovered that the process syslog collector was not running on the electronic security manager. The file system filled up due to stoppage of the process parsetext collector. As a result, there were the three gaps for over 10 hours in logging on certain electronic access control and monitoring devices.

Reliability*First* determined that URE had a violation of CIP-005-3a R3 because it failed to implement its electronic process for monitoring and logging access at access points to the ESP at all times.

Reliability*First* determined the duration of the violation to be from the date the file system stopped collecting logs, through the present.

Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, missing logs increase the likelihood of undetected

and unauthorized access to URE's system. The risk to the reliability of the BPS was mitigated by the following factors. The gap in logs impacted a limited number of devices. For the duration of the violation, there were no cyber security incidents on URE's monitored equipment.

CIP-005-3 R4 (RFC2012011452) and CIP-007-3 R8 (RFC2012011455)

The purpose statement of Reliability Standard CIP-005-3 provides in pertinent part: "Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter."

CIP-005-3 R4 provides:

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

> R4.1. A document identifying the vulnerability assessment process;
>
> R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
>
> R4.3. The discovery of all access points to the Electronic Security Perimeter;
>
> R4.4. A review of controls for default accounts, passwords, and network management community strings;
>
> R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-007-3 provides in pertinent part: "Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-3 R8 provides:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> R8.1. A document identifying the vulnerability assessment process;
>
> R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
>
> R8.3. A review of controls for default accounts; and,
>
> R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-005-3 has a "Medium" VRF and a "Severe" VSL.

URE submitted Self-Reports to Reliability*First* stating that it was in violation of CIP-005-3 R4 and CIP-007-3 R8. URE submitted another Self-Report to Reliability*First* stating that it was in violation of CIP-005-3 R4. During the Compliance Audit, Reliability*First* discovered additional violations of CIP-005-3a R4 and CIP-007-3 R8.

URE performed CVAs for two consecutive years for its electronic access points to the ESP and Cyber Assets within the ESP, but did not have an adequately defined process for performing CVAs. In addition, URE failed to have documentation demonstrating that it included all the following requirements of CIP-005-3 R4 and CIP-007-3 R8 in its CVA: 1) a document identifying the CVA process (CIP-005-3a R4.1 and CIP-007-3 R8.1); 2) a review to verify that it enabled only ports and services required for operations at access points to the ESP (CIP-005-3a R4.2) and for Cyber Assets within the ESP (CIP-007-3 R8.2); 3) the discovery of all access points to the ESP (CIP-005-3a R4.3); 4) a review of controls for default accounts (CIP-005-3a R4.4 and CIP-007-3 R8.3); 5) passwords and network management community strings[4] (CIP-005-3a R4.4); and 6) documentation of the results of the

[4] Community strings are similar to a user identification or password that allows access to a router's or other device's statistics.

assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan (CIP-005-3a R4.5 and CIP-007-3 R8.5).

URE performed CVAs for two consecutive years but failed to conduct a review of controls for network community strings, as required by CIP-005-3a R4.4.

Reliability*First* determined that URE had a violation of CIP-005-3 R4 because it failed to include in its CVA: 1) the required elements for electronic access points to the ESP; and 2) a review of controls for network management community strings. Reliability*First* determined that URE had a violation of CIP-007-3 R8 because it failed to include the required elements in its CVA for Cyber Assets within the ESP.

Reliability*First* determined the duration of the violations to be from the date by which URE was required to conduct a CVA through when URE completed its Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to define and execute an adequate CVA increases the likelihood of compromise to the assets subject to the CVAs. In addition, the lengthy duration of the violation, over two years, increased URE's exposure to this risk.

The risk to the reliability of the BPS was mitigated by the following factors. URE did perform the CVA, and the individuals who performed the assessments can provide supporting details of those assessments. This was a documentation issue where URE failed to retain documentation supporting those details. In addition, for several years, URE configured all access points' network management community strings to be unidirectional (read-only). Furthermore, URE did not use the default values (public or private) for the network management community strings. URE restricted them so they were only accessible by specific internal Cyber Assets, and URE updated them to the latest version.

CIP-006-1 R1; R1.1 (RFC2012011568)

The purpose statement of Reliability Standard CIP-006-1 R1 provides in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R1 provides in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-006-1 R1. URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-006-1 R1. Reliability*First* consolidated the two instances of noncompliance into RFC2012011568. First, URE discovered a five-foot by 18-inch opening in the six-wall border above the suspended ceiling of a PSP at a generating facility. Second, URE maintains one ESP at a generating station with assets in multiple PSPs. URE discovered that the wiring connecting the Cyber Assets in discrete PSPs is not protected by a six-wall boundary such as conduit. URE submitted a Technical Feasibility Exception (TFE) for this issue, which was approved.

Reliability*First* determined that URE had a violation of CIP-006-1 R1 because it failed to ensure all Cyber Assets within an ESP reside within an identified PSP.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Regarding the gap in the six-wall border, there are additional protections in place for the CCAs. The gap in the PSP would only allow access to a hallway within the PSP where no CCAs reside. In order to access the CCAs, an individual would need to access an additional door with a card reader. Regarding the exposed wiring, the assets and the wiring are located within a restricted access site that is manned 24 hours a day. In addition, URE has cameras in place, as well as physical personnel presence, for monitoring of the site at all times.

CIP-006-1 R2; R2.2 (RFC2012011569)
CIP-006-1 R2 provides in pertinent part:

> R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> ***
>
> R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
>
> ***

CIP-006-1 R2 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-006-1 R2. URE submitted another Self-Report to Reliability*First* stating that it was in violation of CIP-006-1 R2. Reliability*First* incorporated both instances of noncompliance into RFC2012011569.

URE discovered that it did not identify its physical access control system (PACS) intelligent controllers as Cyber Assets that authorize and/or log access to the PSP. As a result, URE failed to provide certain protective measures to these devices, as required by CIP-006-1 R2.2. URE also failed to provide the protective measures of CIP-003 R6, CIP-004 R3 and R4, CIP-007, CIP-008, and CIP-009.

In addition, URE installed two servers, which are Cyber Assets that authorize and/or log access to the PSP. URE failed to afford the protective measures of CIP-007-3 R6 to these devices by failing to install the required logging and monitoring software agent on these servers. URE enabled the devices to log all possible events, which resulted in a large number of events generated on these servers. Because URE did not install the required software agent, the logs were being overwritten in less than 24 hours, so URE was unable to review the logs manually. As a result, these servers did not provide security logs for URE's review, and URE did not retain these logs for 90 calendar days, as required by CIP-007-3 R6.

Reliability*First* determined that URE had a violation of CIP-006-1 R2 because it failed to afford certain protective measures to Cyber Assets that authorize and/or log access to the PSP.

Reliability*First* determined the duration of the first instance of the violation to be from the date URE was required to comply with CIP-006-2 for the PACS intelligent controllers, through when URE completed its Mitigation Plan. Reliability*First* determined the duration of the second instance of the violation to be from the date URE installed the servers, through the date URE installed logging and monitoring software.

Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to protect the system intelligent controllers increased the likelihood of compromise of the administrative workstation. Also, failure to protect the servers increased the likelihood of an undetected incident. Furthermore, the duration of the violation increased URE's exposure to this risk. The risk to the BPS was mitigated by the following factors. Regarding the logging and monitoring software on the servers, the PACS has additional network-based monitoring systems in place that log network activity such as the intrusion detection system and the PACS network access point firewalls, all of which send their logs to the security information and event management system where security analysts monitor them. Unauthorized traffic would have had to bypass the intrusion detection system and the firewalls prior to attempting to compromise the servers. In addition, both servers had the required malware prevention software installed. This software reports threats to the enterprise malware prevention console software which, in turn, sends the events to the security information and event management system.

CIP-007-1 R1; R1.1 (RFC2013012114)

The purpose statement of Reliability Standard CIP-007-1 R1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-1 R1 provides in pertinent part:

> R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

***

CIP-007-1 R1 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, Reliability*First* discovered that URE had a violation of CIP-007-1 R1. Reliability*First* determined that URE's cyber security test procedures for new Cyber Assets and significant changes to existing Cyber Assets within the ESP were inadequate. For example, the test plan descriptions and results of testing did not reflect testing of cyber security controls. In addition, URE had change control tickets documenting that testing personnel answered certain questions during the change process, but URE did not provide evidence that the testing prevented adverse effects on cyber security controls. As a result, 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.

In addition, Reliability*First* determined that URE conducted cyber security testing for software changes or upgrades in the production environment utilizing an approach that does not minimize adverse effects on the production environment. URE, using the "rolling wave" method, performed cyber security testing for software changes and upgrades on the assets that are less critical first, followed by a time period (usually 24 hours) to verify successful deployment prior to continuing deployment to assets that are more critical. This approach did not adequately minimize adverse effects on the production system or its operation, as required by CIP-007-3 R1.1, because untested upgrades may contaminate the environment.

Reliability*First* determined that URE had a violation of CIP-007-1 R1 because URE failed to: 1) ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls; and 2) implement cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk to the reliability of BPS, but did not pose a serious or substantial risk. Specifically, testing security controls on a CCA after making a change to the system is crucial. Without such testing, the change to the system could introduce an unknown vulnerability to the system. In addition, the lengthy duration of the violation increased URE's exposure

to this risk. The risk to the reliability of the BPS was mitigated by the following factors. URE's process made the change approvers aware of the impact the change would have and allowed them to approve or deny the change request accordingly. In addition, URE used a process where any changes to firewall rules required the justification to be added as a comment to the rule set along with a reference to the associated change ticket number. URE also leveraged the annual CVA process to test all cyber security controls and confirm that it had documented any changes since the prior year through change tickets. As a result, although URE's change control process was inadequate, URE had a functioning change control process.

In addition, the ESP and PACS environments have additional network-based monitoring systems in place that log network activity, such as the intrusion detection system (IDS) and network access point firewalls, all of which send their logs to the security monitoring system where security analysts monitor them. Any undetected compromise of these systems would have had to bypass the IDS and the firewalls prior to attempting to compromise Cyber Assets within these environments. All URE's operating system servers and workstations have the required malware prevention software installed. The malware prevention software is configured to report threats to the enterprise malware prevention console software, which in turn sends the events to the security monitoring system. All devices in these environments have security patches applied in accordance with the URE patch management program. Furthermore, URE's vendor tests for functionality issues and only provides updates that pass its testing process. URE has not experienced any security issues resulting from the "rolling wave" approach.

CIP-007-1 R2 (RFC2013011942)

CIP-007-1 R2 provides:

> R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> > R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
> >
> > R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R2 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-007-1 R2. During the Compliance Audit, Reliability*First* discovered an additional instance of a violation of CIP-007-1 R2 for URE. During URE's CVA, URE performs a detailed ports and services assessment to ensure that only those ports and services necessary for secure operation are enabled. The resulting annual CVA becomes the new baseline for ports and services. However, URE did not maintain this baseline configuration between annual CVAs. As a result, ports and services could have been modified without authorization since the last cyber CVA without detection since URE restarts the baseline each year.

During URE's CVA for a specific year, URE identified that several of its open ports and services were not justified as being required for normal and emergency operations. URE discovered these open ports and services because the third-party contractor that performed URE's CVA utilized an improved tool. For the majority of the open ports and services, URE obtained justification that they were required for normal and emergency operations. URE has documented confirmation that it should disable seven of these open ports and services.

In addition, URE's list of ports and services did not document individually or by specified grouping which ports and services should be enabled or listening on which devices.

Reliability*First* determined that URE had a violation of CIP-007-1 R2 because it failed to implement its process to ensure that only those ports and services required for normal and emergency operations are enabled as related to securing those systems determined to be CCAs.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, to the present.

Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to protect Cyber Assets within the ESP through a ports and services baseline increases the likelihood of a security gap. In addition, the lengthy duration of the violation increased URE's exposure to this risk. The risk to the BPS was mitigated by the following factors. Although URE failed to maintain the ports and services baselines, each change to ports and services required prior approval through the change control process. URE utilized these

change tickets to request, authorize, and document ports and services changes between CVAs. The annual CVA change ticket assessments did not identify any unauthorized enabled ports and services. In addition, URE's change control process included questions related to the impact on ports and services for a given change, and allowed approvers to approve or deny the change request accordingly.

Furthermore, the ESP and PACs environments have additional network-based monitoring systems in place that log network activity, such as the IDS and network access point firewalls, all of which send their logs to the security monitoring system where security analysts monitor them. Any undetected compromise of these systems would have had to bypass the IDS and the firewalls prior to attempting to compromise Cyber Assets within these environments. All Windows servers and workstations have the required malware prevention software installed. The malware prevention software is configured to report threats to the enterprise malware prevention console software, which in turn sends the events to the security monitoring system. All devices in these environments have security patches applied in accordance with the URE patch management program.

Regarding URE's open ports and services, the devices are not connected to the business local area network or the Internet. The devices were all located within an ESP and PSP with an additional firewall present between the devices and URE's system, and as a result, extra credentials were required to access these devices.

CIP-007-1 R3 (RFC2013011943)
CIP-007-1 R3 provides:

> R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
>
> > R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
> >
> > R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R3 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-007-3 R3. During the Compliance Audit, Reliability*First* discovered an additional instance of a violation of CIP-007-1 R3 for URE. URE evaluated security patches released from its vendor within 30 days of release from the vendor. However, URE should have been assessing security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades from the application vendor. In addition, URE provided insufficient evidence that its vendor was in fact performing assessments of these patches. Instead, URE provided evidence that its vendor was testing the patches but not assessing them for applicability.

In addition, Reliability*First* discovered that URE's security patch implementation did not address software patch updates beyond security patches for certain software. For example, URE does not assess and implement security patches.

Reliability*First* determined that URE had a violation of CIP-007-1 R3 because it failed to implement its security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches.

Reliability*First* determined the duration of the violation to be from the date by which URE was required to comply with CIP-007-1 through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to document the assessment of security patches and upgrades increases the likelihood of inadequately protecting Cyber Assets. In addition, the lengthy duration of the violation increased URE's exposure to this risk. The risk to the reliability of the BPS was mitigated by the following factors. Regarding URE's assessment of security patches, URE performed assessments of security patches, although at an interval greater than 30 days. In addition, the devices were all located within an ESP and PSP, and as a result, extra credentials were required to access these devices.

Regarding URE's security patch implementation, the accounts at issue do not have direct outward facing access to the corporate business network or to the Internet, reducing the likelihood of access from outside the network.

CIP-007-1 R4 (RFC2013011945)

CIP-007-1 R4 provides in pertinent part:

> R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
>
> ***
>
> R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

CIP-007-1 R4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-007-3 R4. The anti-virus and malware prevention signatures on URE's voltage regulators for its generating stations were not up to date or available, as required by CIP-007-3 R4.2. Although these voltage regulators are technically incapable of running anti-virus and malware prevention tools, URE failed to submit a TFE.

During the Compliance Audit, Reliability*First* discovered an additional instance of non-compliance with CIP-007-1 R4 for URE. Reliability*First* discovered that URE , using the "rolling wave" approach, performs testing and implementing for updated signature files on the assets that are less critical first, followed by a time period (usually 24 hours) to verify successful deployment prior to continuing deployment to assets that are more critical. This approach places the signatures into the production environment prior to testing, and as such does not adequately address testing of anti-virus and malware prevention signatures, as required by CIP-007-3 R4.2.

Reliability*First* determined that URE had a violation of CIP-007-1 R4 because it failed to: 1) implement its process for testing anti-virus and malware preventions signatures; and 2) implement its process for the update of anti-virus and malware prevention signatures.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of BPS, but did not pose a serious or substantial risk. Specifically, the "rolling wave" approach increases the likelihood of compromise to Cyber Assets within the production environment. In addition, the lengthy duration of the violation increased URE's exposure to this risk. The risk to the reliability of the BPS was mitigated by the following factors. Regarding the voltage regulator devices, the devices are located within an ESP and PSP and additional credentials are required to gain access to this device. In addition, the site has restricted access and is manned at all times. Regarding testing of the signatures, URE installed anti-virus software and has not experienced any security issues resulting from the "rolling wave" approach.

CIP-007-1 R5 (RFC2012011453)

CIP-007-1 R5 provides in pertinent part:

> R5. Account Management — The Responsible Entity shall 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.
>
> ***
>
> R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
>
> > R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.
> >
> > R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.
> >
> > R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
>
> ***

CIP-007-1 R5 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-007-3 R5. For one shared account, URE limited access to three individuals who typically use their own separate laptop to log into the account. URE traced the usage of the shared account through the unique IP address of the specific user. However, URE discovered that a user may access another user's laptop to log into the account, thereby rendering the account use untraceable. Therefore, URE failed to implement an audit trail of the account use for this account, as required by CIP-007-3 R5.2.3.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-007-3 R5. Specifically, URE does not have evidence of audit trails of individual user account activity for its generating station voltage regulators. For certain devices, URE did not review logs, and for other devices, such logs are unavailable. Therefore, URE failed to implement its policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts, as required by CIP-007-3 R5.2.

During the Compliance Audit, Reliability*First* discovered another instance of non-compliance with CIP-007-3 R5. Reliability*First* discovered that for several shared accounts that URE could have renamed, URE failed to do so, as required by CIP-007-3 R5.2.1. For example, URE failed to rename the administrator accounts for certain devices. In addition, Reliability*First* discovered that URE could not provide sufficient evidence of individual access to shared accounts, as required by CIP-007-3 R5.2.2.

Reliability*First* determined that URE had a violation of CIP-007-3 R5 because it failed to: 1) establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of certain individual user account access activity for a minimum of 90 days; 2) implement its policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges, including factory default accounts; and 3) have in place an audit trail of the account use for one shared account.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through the present.

Reliability*First* 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 failure to rename administrator accounts poses a risk to the reliability of the BPS by providing a potential intruder with part of the login information to an account that can perform administrator tasks on the system. This increases the likelihood of compromise to BPS reliability. The risk to the reliability of the BPS was mitigated by the following factors. Regarding the failure to rename administrator accounts, the accounts at issue do not have direct outward facing access to the corporate business network or to the internet, reducing the

likelihood of access from outside the network. URE restricts all physical access to Cyber Assets to individuals with valid personnel risk assessments (PRAs) and annual cyber security training.

Regarding the voltage regulator devices, the devices are located within an ESP and PSP, which means additional credentials are required to gain access to this device. In addition, the site has restricted access and is manned at all times.

Regarding the audit trail of the shared account, the three individuals had authorized access to the shared account and had valid PRAs and cyber security training during the time period of the violation. In addition, URE experienced no cyber security events during the time period of the violation, and URE did not need to call upon the audit trail for this account.

CIP-007-1 R6; R6.3, R6.4, R6.5 (RFC2012011454 and RFC2013013118)

CIP-007-1 R6 provides in pertinent part:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> > R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
> >
> > R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
> >
> > R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-1 R6 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating it was in violation of CIP-007-3 R6 (RFC2012011454). Specifically, URE discovered that monitoring was temporarily disabled on five Cyber Assets within the ESP.

During the Compliance Audit, Reliability*First* discovered that URE had several devices configured to the security information and event management system that were technically incapable of performing monitoring or generating logs. URE failed to submit a TFE for these devices.

URE submitted another Self-Report to Reliability*First* stating it was in violation of CIP-007-3 R6 (RFC2013013118). During a routine log review, URE discovered that the collection Internet Protocol address for one aggregate switch was misconfigured. As a result, URE failed to review logging for the switch due to lack of log data.

URE submitted another Self-Report to Reliability*First* stating it was in violation of CIP-007-3 R6 (consolidated into RFC2013013118). During an unplanned outage of URE's security manager security information and event management tool, URE discovered that for several devices, messages pertaining to denied firewall traffic were not collected because of the inadequacy of the frequency at which log buffers can send logging information to a collection device.

Reliability*First* determined that URE had a violation of CIP-007-1 R6 because it failed to monitor continuously the activity on all its Cyber Assets or submit a TFE where appropriate.

Reliability*First* determined the duration of the violation RFC2012011454 to be from when URE was required to submit a TFE through when URE completed its Mitigation Plan. Reliability*First* determined the duration of the violation RFC2013013118 to be from the date the Standard became mandatory and enforceable on URE through the present.

Reliability*First* 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 separate instances of noncompliance making up this violation resulted in multiple vulnerabilities on URE's system. The risk to the reliability of the BPS was mitigated by the following factors. URE controls physical access to the devices through a key management program. URE had the following security measures in place: 1) the cabinet doors that contain the devices are protected by alarm, and URE security personnel monitors them 24 hours a day; 2) all personnel with physical and/or logical access have valid PRAs and cyber security training; 3) the single default local administrator account is disabled; 4) the devices are physically stored in a controlled access PSP, and network intrusion detection is active and monitoring for anomalous traffic; 5) URE's passwords for these devices meet or exceed the CIP password complexity and change requirements; and 6) URE has installed, maintained, and monitored anti-virus on all operating system servers and workstations.

Regarding the voltage regulator devices, the devices are located within an ESP and PSP, and additional credentials are required to gain access to this device. In addition, the site has restricted access and is manned 24 hours a day. Regarding the aggregate switch, URE's system segments traffic from the aggregate switch feeder systems, which gather data to be published as view-only on the server. As a result, the loss of this traffic does not affect BPS operation. Regarding the affected devices, the loss of logging information does not directly affect BPS operation but instead provides insight into the traffic flowing across the network.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, Reliability*First* has assessed a penalty of seventy-five thousand dollars ($75,000) for the referenced violations. In reaching this determination, Reliability*First* considered the following factors:

1. URE's violation history, which was considered an aggravating factor in penalty assessment;
2. URE self-reported the violations, except for the CIP-007-1 R1.1 violation;[5]
3. URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which Reliability*First* considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. URE committed to performing above-and-beyond activities to implement reliability enhancements that exceed those actions that would achieve and maintain baseline compliance with the NERC CIP Reliability Standards and Requirements, as described below;
8. When considered as an aggregate, the instant violations posed an elevated level of possible risk to URE's Cyber Assets, which was indicative of programmatic failure; and
9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[5]URE historically engages in rigorous self-assessments, the result of which are robust Self-Reports and rigorous mitigating activities. While URE failed to timely detect many of these issues, URE's historic compliance performance demonstrates its commitment to spontaneous timely detection and timely correction unconnected to a pending regional compliance monitoring action.

URE committed to collaborating with Reliability*First* to perform the following above-and-beyond activities to implement reliability enhancements. Specifically, URE agreed to perform certain actions to improve its capability and performance in key management practices of asset and configuration management, verification, and validation.

Based on information provided by URE throughout the Compliance Audit and enforcement process, Reliability*First* analyzed the root cause and risk severity of the instant violations and determined that if URE had high capability and performance in certain key management practices, the number and severity of URE's violations may have been reduced. First, high capability and performance in asset and configuration management would impact compliance with many of the Requirements at issue in the violations. When implementing asset and configuration management programs, entities establish an inventory of assets and configurable items, define the attributes of those assets and configurable items, and maintain their integrity in the context of reliability and resilience. The violations impacted by these activities are the violations related to asset identification (CIP-006 R2.2), CVAs (CIP-005 R4 and CIP-007 R8), and Cyber Asset change control and configuration management (CIP-005 R2.2 and CIP-007 R1, R3, R4 R5, and R6).

Second, high capability and performance in validation and verification activities would impact compliance with many of the Requirements at issue in the violations. Validation activities confirm that changes to the systems comprising the BPS function as designed in the intended environment and conditions before the changes are made operational. Verification activities confirm that any changes to the systems comprising the BPS and affecting its reliability are conducted in accordance with requirements, plans, or specifications. URE performed cyber security functions separately for its affected and business units, which resulted in numerous violations (CIP-005 R2 and R4 and CIP-007 R1, R2, R3, R4, R5, and R8). These violations include processes that involve the testing and validation of electronic access, software upgrades, secure ports and services, patch updates, malware updates, valid accounts, and properly assessed cyber vulnerabilities. All of these are testing and validation processes, thereby demonstrating improvement opportunities in validation and verification.

These key management practice areas (asset and configuration management, validation, and verification) are correctly mapped to the root causes of the identified violations and constitute areas for improvement. URE completed the mitigating actions set forth below for each violation, and those mitigating actions resulted in a baseline level of internal controls sufficient to return URE to compliance with the Requirements at present and prevent recurrence of the same noncompliance. However, URE and Reliability*First* determined that improving URE's capability and performance in the identified key management practices would lead to improved grid reliability and resilience and institute a higher level

of preventative internal controls that may further prevent noncompliance with a wider array of Requirements.

To that end, URE agreed to collaborate with Reliability*First* to undertake the actions set forth below in order to improve its capability and performance in these key management practices of asset and configuration management, verification, and validation. Such process improvements, when fully implemented, will positively impact compliance with the Requirements that constitute the majority of the violations at issue in this Agreement and will result in holistic improvement to grid reliability and resiliency.

By analyzing the root causes of its violations and surveying available frameworks, URE agreed to utilize the SANS Institute's 20 Critical Controls for Effective Cyber Defense (SANS 20) in effect at the time of the Settlement Agreement, to develop and implement an internal controls framework related to frequently-violated, high-risk Requirements. The SANS 20 are critical controls for effective cyber defense, developed originally by the National Security Agency (NSA) and the SANS Institute to "share [the NSA's] attack information to provide … control-prioritization knowledge for civilian government agencies and critical infrastructure."[6] The SANS 20 methodology is a "living" document that changes based on the most relevant threat information identified by multiple experts and agencies and based on actual attacks and effective defenses.[7]

The SANS 20 supports cyber security and reliability capability and performance, and its goals align with the goals of the CIP Requirements as well as asset and configuration management. The goal of the SANS 20 is to "protect critical assets, infrastructure, and information by strengthening [an] organization's defensive posture through continuous, automated protection and monitoring of sensitive information technology infrastructure to reduce compromises, minimize the need for recovery efforts, and lower associated costs."[8] Similarly, the CIP Requirements aim to protect critical infrastructure by, among other things, implementing the continuous, automated protection and monitoring on high-value assets and configurable items, as described in the SANS 20 and identified by the asset and configuration management practice. Mapping the SANS 20 to the Requirements is therefore a worthwhile endeavor because it can assist URE and other Registered Entities with implementing robust cyber security that meaningfully impacts grid reliability. Rather than implementing an internal controls framework in a vacuum, or an internal controls framework related

[6] *A Brief History of the 20 Critical Cyber Controls*, available at http://www.sans.org/critical-securitycontrols/history.php.

[7] *Critical Controls for Effective Cyber Defense, Version 4.1* (March, 2013), available at http://www.sans.org/critical-security-controls/guidelines.php, at 2.

[8] *Id*.

to the CIP Requirements as they stand at a given point in time, URE will leverage the work of experienced agencies and organizations to improve grid reliability and resilience through robust cyber security.

In recognition of improvement opportunities in the asset and configuration management practice, URE will have documented risks and associated detective, corrective, and preventive internal controls to address three CIP Requirements related to asset and configuration management that URE has frequently violated and that represent high risk to the BPS (CIP-007-1 R1, R2, and R6). URE will provide its risk assessment methodology and the results of the risk assessment to Reliability*First*.

URE will include an analysis of the SANS 20 in its development and assessment of its internal control framework. URE will have provide a mapping between the SANS 20 and the CIP Requirements. URE will have develop, assess and test internal controls for CIP-007-1 R1, R2, and R6, and prioritized by risk to grid reliability the internal control is designed to mitigate. URE will provide quarterly updates to Reliability*First* regarding its development and implementation of the internal control framework. This assist visit will include assessment of the internal controls framework, its impact on grid reliability, and its impact on compliance with the identified Requirements.

Pursuant to URE's goal of improving its asset and configuration management especially related to CIP-007 R1, R2, and R6, Reliability*First* will conduct an assist visit with URE to review URE's capability and performance in asset and configuration management.

To focus on improvement opportunities in the validation and verification practices, URE is implementing a holistic approach to company-wide cyber security and reliability. In recognition that many of the violations resulted from divergent approaches to cyber security in various units, URE will implement a company-wide CIP program by integrating its divergent units' programs into one program. In addition, URE will put tools in place to improve its capability and performance in validation and verification of cyber security tasks important for grid reliability and resilience.

URE will implement a company-wide software tool that will assist with its validation and verification internal controls, including: 1) linkage to the internal controls framework (both a validation and verification activity); 2) reminders to perform periodic tasks (a verification activity); 3) awareness checks regarding activities related to Requirements (a validation activity); and 4) facilitation of compliance submittal management (a validation activity).

URE will evaluate the Mitigation Plans at issue in this Settlement Agreement to determine their alignment with the program. URE will provide Reliability*First* with a preliminary outline of reliability

risk areas relative to its CIP compliance program, capturing aspects of a risk assessment to be performed by a third-party consultant. Reliability*First* will provide feedback to URE regarding the outline, such that final scoping of the third-party risk assessment will be completed. URE will develop a plan to integrate all its business units' assets into one program to create a single, company-wide CIP program. In doing so, URE will undertake the integration by prioritizing its activities from highest to lowest risk to BPS reliability.

Reliability*First* and URE will work together to determine the scope of a Reliability*First*-led assist visit that will be most useful for URE to evaluate its company-wide CIP program. Reliability*First* will conduct an assist visit with URE to review URE's capability and performance in management practice areas related to the integration plan, including but not limited to validation and verification, to ensure their effectiveness for grid reliability and resilience. URE will provide Reliability*First* with an explanation of how it will incorporate the results from Reliability*First*'s assist visit and the third-party contractor's risk assessment into the implementation of its single company-wide CIP program. URE will complete the integration of the CIP program into the CIP program to create a single company-wide CIP program.

After consideration of the above factors, Reliability*First* determined that, in this instance, the penalty amount of seventy-five thousand dollars ($75,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[9]

CIP-005-1 R2 (RFC2013011941)
URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008835-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. define a dynamic ports and services process;
2. enhance its change control process;
3. issue documentation update;
4. perform training for relevant personnel;

[9] *See* 18 C.F.R § 39.7(d)(7).

5. aggregate running ports and services on devices at issue;
6. compile a list of unjustified ports and services;
7. obtain justification for or disable all unjustified ports and services;
8. disable any unjustified ports and services; and
9. update process documentation to include the ports and services methodology for justification of ports and services.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*.

CIP-005-3a R3; R3.2 (RFC2013012708)

URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT009920 and was submitted as non-public information to FERC in accordance with FERC orders. URE requested a Mitigation Plan completion date extension, which was granted by Reliability*First*.

URE Mitigation Plan requires URE to:

1. develop and implement system-compatible backup logging;
2. develop and document a process for maintenance and testing of the backup logging solution; and;
3. train applicable personnel on the process.

CIP-005-3a R4 (RFC2012011452)

URE's Mitigation Plan to address its violation of CIP-005-3a R4 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008887-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. complete the CVAs at issue by hiring a third party that specializes in such assessments to conduct reviews;

2. update the CVA procedure to ensure the documented results align with each relevant CIP Requirement; and
3. update the vulnerability management program to include the missing network management community strings controls testing requirement.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*. After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R8 (RFC2012011455)

URE's Mitigation Plan to address its violation of CIP-007-3 R8 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008888-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. complete the affected CVAs by hiring a third party that specializes in such assessments to conduct reviews;
2. update the CVA procedure to ensure the documented results align with each relevant CIP Requirement; and
3. update the vulnerability management program to include the missing network management community strings controls testing requirement.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*. After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-006-1 R1 (RFC2012011568)

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT009390 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. hire a construction firm to seal the opening above the suspended ceiling to the underside of the roof deck;
2. develop a preventative maintenance procedure for performing an annual assessment and to spot check boundaries periodically when there are construction activities in the area; and
3. submit a TFE for the issue with the exposed conduit.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*. After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-006-1 R2; R2.2 (RFC2012011569)

URE's Mitigation Plan to address its violation of CIP-006-1 R2 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT009265-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform an assessment and develop a document to identify the pertinent details for the intelligent controllers and associated information related to the PSP;
2. determine the technical capabilities of the intelligent controllers;
3. determine that it would submit TFEs for the intelligent controllers;
4. perform security capabilities testing on the intelligent controllers;
5. add the intelligent controllers associated with PSPs to the change and configuration management database;
6. update device configuration;
7. complete migration to the correct group at URE;
8. install the required logging and monitoring software agent on the servers; and
9. validate that both systems are sending all applicable security logs to the monitoring system.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*. After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-1 R1; R1.1 (RFC2013012114)

URE Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT009538 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform an exhaustive discovery of open ports and services, all accounts, Cyber Assets, applicable antivirus and malware signatures, and configuration baselines;
2. develop tools to automate discovery of local accounts, ports and services, registry settings, and simple network management protocol community strings;
3. define the scope of applicable security-related registry settings, and maintain monitoring of applicable security-related registry settings;
4. evaluate third-party vendor security testing for quality of evidence and test environment representative of production environment;
5. document the rolling wave approach and provide detail on devices in first wave and subsequent waves;
6. revise URE's procedure for process documentation to incorporate a cross-department peer review of CIP procedures;
7. commit to define dynamic ports and services process;
8. enhance the change control process;
9. issue documentation updates; and
10. perform communication and training to applicable personnel.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*.

CIP-007-1 R2 (RFC2013011942)

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008836-3 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. implement a service contract to provide support for applicable devices;
2. implement the vendor solution;
3. disable non-required ports and services;
4. create a job aid for adding devices into the ESP;
5. update process documentation to include methodology for justification of ports and services;
6. define dynamic ports and services process;
7. enhance the change control process and issue documentation updates; and
8. perform training for applicable personnel.

CIP-007-1 R3 (RFC2013011943)

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to Reliability*First*. URE submitted a revised Mitigation. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008837-2 and was submitted as non-public information to FERC on in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop a comprehensive list of all applications, network devices, and operating systems in use within the ESP;
2. develop a process for managing multiple vendor updates, within the specified periodicity, including controls to ensure that URE receives, documents, and tracks notifications;
3. update Cyber Assets with applicable patches; and
4. conduct training and implementation of the process for managing multiple vendor updates.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*.

CIP-007-1 R4 (RFC2013011945)

URE's Mitigation Plan to address its violation of CIP-007-1 R4 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008883-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. evaluate third-party vendors' anti-virus and malware testing for quality of evidence and test environment representative of URE's environment;
2. document the rolling wave approach and provide detail on the devices in the first wave and subsequent waves;
3. revise URE's procedure for process documentation to incorporate a cross-department peer review of CIP procedures;
4. implement a service contract with the vendor to provide support for the voltage regulator devices;
5. implement the solution provided by the vendor; and
6. create a job aid for adding devices to the ESP.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*.

CIP-007-1 R5 (RFC2012011453)

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008889-2 and was submitted as non-public information to FERC in accordance with FERC orders. URE requested a Mitigation Plan completion date extension, which was granted by Reliability*First*.

URE's Mitigation Plan requires URE to:

1. create and implement a process for managing a manual log;
2. update procedure controls to specific log requirements for shared administrator accounts;

3. review the change control process and identify specific measures for renaming of admin accounts prior to production implementation;
4. update process documentation to address measures for renaming of admin accounts prior to production implementation;
5. execute a service contract with its vendor;
6. implement the software solution provided by the vendor;
7. create a job aid for adding devices into the ESP;
8. perform an exhaustive discovery of all accounts and where they are used;
9. develop tools to automate discovery of local accounts;
10. rename or remove privileged accounts, where feasible;
11. identify and implement tools for managing and reporting access;
12. create a policy for managing and reporting access to accounts that cannot be renamed; and
13. update governing procedure with detailed methods, process flows, and question and answer checklists.

CIP-007-1 R6 (RFC2012011454)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008886-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE Mitigation Plan required URE to submit a TFE, which was approved by Reliability*First*.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*. After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-1 R6 (RFC2013013118)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT010169 and was submitted as non-public information to FERC in accordance with FERC orders. URE requested a Mitigation Plan completion date extension, which was granted by Reliability*First*.

URE's Mitigation Plan requires URE to:

1. verify that all network devices are communicating with URE's electronic security manager or submit a TFE;
2. develop and document a process to set and validate device and collector configurations for logging;
3. train applicable personnel on the process; and
4. submit a TFE.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[10]

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,[11] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on January 14, 2014. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of a seventy-five thousand dollar ($75,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. URE violation history, which was considered an aggravating factor in penalty assessment;
2. URE self-reported most of the violations, as discussed above;
3. Reliability*First* reported that URE was cooperative throughout the compliance enforcement process;

[10] *See* 18 C.F.R. § 39.7(d)(4).

[11] *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).

4. URE had a compliance program at the time of the violation which Reliability*First* considered a mitigating factor, as discussed above;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. Reliability*First* determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. URE committed to performing above-and-beyond activities to implement reliability enhancements that exceed those actions that would achieve and maintain baseline compliance with the NERC CIP Reliability Standards and Requirements, as discussed above;
8. Reliability*First* considered that all the instant violations, as an aggregate, posed an elevated level of possible risk to URE's Cyber Assets, which was indicative of programmatic failure; and
9. Reliability*First* reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of seventy-five thousand dollars ($75,000) 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.

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the attached documents are deemed confidential by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be Included as Part of this Notice of Penalty

The attachments to be included as part of this Notice of Penalty are the following documents:

a) Settlement Agreement by and between Reliability*First* and URE, included as Attachment a;

b) Record documents for the violation of CIP-005-1 R2, included as Attachment b:
   1. URE's Self-Report;
   2. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;
   3. URE's Mitigation Plan designated as RFCMIT008835-2;
   4. URE's Certification of Mitigation Plan Completion;

c) Record documents for the violation of CIP-005-3a R3, included as Attachment c:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as RFCMIT009920;

d) Record documents for the violation of CIP-005-3 R4 and CIP-007-3 R8, included as Attachment d:
   1. URE's Self-Report;
   2. URE's Self-Report;
   3. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form ;
   4. URE's Mitigation Plan to address CIP-005-3 R4 designated as RFCMIT008887-2;
   5. URE's Certification of Mitigation Plan Completion;
   6. Reliability*First*'s Verification of Mitigation Plan Completion;
   7. URE's Mitigation Plan to address CIP-0070-3 R8 designated as RFCMIT008888-1;
   8. URE's Certification of Mitigation Plan Completion;
   9. Reliability*First*'s Verification of Mitigation Plan Completion;

e) Record documents for the violation of CIP-006-1 R1, included as Attachment e:
   1. URE's Self-Report;

2. URE's Self-Report;
3. URE's Mitigation Plan designated as RFCMIT009390;
4. URE's Certification of Mitigation Plan Completion;
5. Reliability*First*'s Verification of Mitigation Plan Completion;

f) Record documents for the violation of CIP-006-1 R2, included as Attachment f:

1. URE's Self-Report;
2. URE's Self-Report;
3. URE's Mitigation Plan designated as RFCMIT009265-1;
4. URE's Certification of Mitigation Plan Completion;
5. Reliability*First*'s Verification of Mitigation Plan Completion;

g) Record documents for the violation of CIP-007-1 R1, included as Attachment g:

1. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;
2. URE's Mitigation Plan designated as RFCMIT009538;
3. URE's Certification of Mitigation Plan Completion;

h) Record documents for the violation of CIP-007-1 R2, included as Attachment h:

1. URE's Self-Report;
2. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;
3. URE's Mitigation Plan designated as RFCMIT008836-3;

i) Record documents for the violation of CIP-007-1 R3, included as Attachment i:

1. URE's Self-Report;
2. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;
3. URE's Mitigation Plan designated as RFCMIT008837-2;
4. URE's Certification of Mitigation Plan Completion;

j) Record documents for the violation of CIP-007-1 R4, included as Attachment j:

1. URE's Self-Report;
2. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;

3. URE's Mitigation Plan designated as RFCMIT008883-1;
4. URE's Certification of Mitigation Plan Completion;

k) Record documents for the violation of CIP-007-1 R5, included as Attachment k:

1. URE's Self-Report;
2. URE's Self-Report;
3. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;
4. URE's Mitigation Plan designated as RFCMIT008889-2;

l) Record documents for the violation of CIP-007-1 R6 (RFC2012011454), included as Attachment l:

1. URE's Self-Report;
2. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form ;
3. URE's Mitigation Plan designated as RFCMIT008886-2;
4. URE's Certification of Mitigation Plan Completion;
5. Reliability*First*'s Verification of Mitigation Plan Completion;

m) Record documents for the violation of CIP-007-1 R6 (RFC2013013118), included as Attachment m:

1. URE's Self-Report;
2. URE's Self-Report ; and
3. URE's Mitigation Plan designated as RFCMIT010169.

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Robert K. Wargo* Director of Analytics & Enforcement Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542 (330) 456-2488 (330) 456-5408 - facsimile bob.wargo@rfirst.org Niki Schaefer* Managing Enforcement Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542 (330) 456-2488 (330) 456-5408 - facsimile niki.schaefer@rfirst.org	Sonia C. Mendonça* Assistant 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* North American Electric Reliability Corporation Senior Counsel and Associate Director, Enforcement Processing 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net L. Jason Blake* General Counsel Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542 (330) 456-2488 (330) 456-5408 – facsimile jason.blake@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

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

Respectfully submitted,

/s/ Sonia Mendonça

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

Sonia C. Mendonça
Assistant 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
North American Electric Reliability Corporation
Senior Counsel and Associate Director, Enforcement Processing
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

Attachments