NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

July 31, 2014

VIA ELECTRONIC FILING

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

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entities
FERC Docket No. NP14-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), Unidentified Registered Entity 2 (URE2), Unidentified Registered Entity 3 (URE3), Unidentified Registered Entity 4 (URE4), Unidentified Registered Entity 5 (URE5), Unidentified Registered Entity 6 (URE6) and Unidentified Registered Entity 7 (URE7) (collectively, the Unidentified Registered Entities), NERC Registry IDs# NCRXXXXX1, NCRXXXXX2, NCRXXXXX3, NCRXXXXX4, NCRXXXXX5, NCRXXXXX6, and NCRXXXXX7, 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]

The Unidentified Registered Entities are URE Parent Company Corp. (URE Parent Company) affiliated registered entities.

[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 (2011). *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).

This Notice of Penalty is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and the Unidentified Registered Entities have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the thirty-five violations[3] of CIP-003, CIP-004, CIP-005, CIP-007, and CIP-009. According to the Settlement Agreement, the Unidentified Registered Entities neither admit nor deny the violations, but have agreed to the assessed penalty of $50,000, 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. The violations identified as NERC Violation Tracking Identification Numbers RFC2012010385, RFC2012010386, RFC2012010387, RFC2012010389, RFC2012010995, RFC2012011061, RFC2012011062, RFC2012011063, RFC2012011064, RFC2012011065, RFC2012011066, RFC2012011067, RFC2012011068, RFC2012011069, RFC2012011070, RFC2012011071, RFC2012011072, RFC2012011073, RFC2012011074, RFC2012011075, RFC2012011076, RFC2012011077, RFC2012011078, RFC2012011099, RFC2012011101, RFC2012011102, RFC2012011123, RFC2012011265, RFC2012011268, RFC2012011270, RFC2012011272, RFC2012011273, RFC2012011443, RFC2012011444, and RFC2012011471 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 executed by and between ReliabilityFirst and the Unidentified Registered Entities. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Registered Entity	Total Penalty
RFC2012011444	CIP-003-2	R6	Lower/Severe	URE1	$50,000

[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.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Registered Entity	Total Penalty

RFC2012011471	CIP-004-1	R2;
		R2.1;
		R2.3
			Lower/
			Severe
				URE6	$50,000

RFC2012010995				URE4	
RFC2012010385	CIP-004-3	R4; R4.2	Lower/ Moderate	URE4	
RFC2012011443				URE3	
RFC2012011272	CIP-005-3a	R1; R1.5	Medium/ Severe	URE7	

RFC2012011061	CIP-005-3	R2;
		R2.1;
		R2.2
			Medium/
			Severe
				URE4	

RFC2012011067				URE5	
RFC2012011123				URE1	
RFC2012011071				URE6	
RFC2012011273	CIP-005-3a	R3; R3.2	Medium/ Severe	URE7	
RFC2012011078	CIP-005-1	R5; R5.2	Lower/ Severe	URE1	
RFC2012011062				URE4	
RFC2012011068				URE5	
RFC2012011072				URE6	
RFC2012010389	CIP-007-3a	R1; R1.1	Medium/ Severe	URE1	
RFC2012011063	CIP-007-1	R1; R1.3	Lower/ Severe	URE4	
RFC2012011069				URE5	

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Registered Entity	Total Penalty
RFC2012011073	CIP-007-1	R1; R1.3	Lower/ Severe	URE6	$50,000
RFC2012011099				URE1	
RFC2012011101	CIP-007-1	R5	Lower/ Severe	URE1	
RFC2012011064				URE4	
RFC2012011074				URE6	
RFC2012011066				URE5	
RFC2012010386	CIP-007-1	R5; R5.3.3	Lower/ Severe	URE2	
RFC2012011077	CIP-007-3a	R5; R5.3.3	Medium/ Severe	URE7	
RFC2012011102	CIP-007-1	R6	Lower/ Severe	URE1	
RFC2012011065				URE4	
RFC2012011070				URE5	
RFC2012011075				URE6	
RFC2012010387	CIP-007-1	R6	Lower/ Severe	URE2	
RFC2012011076	CIP-007-3a	R7; R7.3	Lower/ Severe	URE6	
RFC2012011265	CIP-009-1	R1	Medium/ Severe	URE4	
RFC2012011268				URE5	
RFC2012011270				URE6	

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

Compliance Background

Since the Unidentified Registered Entities' initial compliance date, the seven entities have instituted a model to assign categories of assets to particular URE Parent Company registered entities to gain efficiencies across the organization. Under this model, each shared asset type is assigned to only one registered entity so that a single registered entity retains responsibility for Critical Infrastructure Protection (CIP) compliance of that asset type.

ReliabilityFirst conducted a Compliance Audit (the Compliance Audit). The Settlement Agreement included in this Notice of Penalty resolves violations that were self-reported prior to the Compliance Audit and violations that were discovered during the Compliance Audit.

As a result of the URE Parent Company designation of assigned responsibilities of shared assets, compliance assessments of CIP-006 R2, R4, R5, R6, R7, and R8 were deferred until the subsequent CIP Compliance Audit, which included all URE Parent Company registered entities.[4]

CIP-003-2 R6 (RFC2012011444)

URE1 submitted a Self-Report stating that it was in violation of CIP-003-2 R6. URE1 discovered that it had not identified, controlled, and documented multiple completed software configuration changes on its dial-up service devices pursuant to the URE Parent Company Information Technology (IT) change control process. These devices are dial-up accessible communication processors that provide communication, time synchronization, and data handling capability. Data passes through the communication processor database and it can be retrieved remotely.

ReliabilityFirst determined that URE1 had a violation of CIP-003-2 R6 because it failed to identify, control, and document multiple completed software configuration changes on its devices.

ReliabilityFirst determined the duration of the violation to be from the date URE1 did not identify, control or document the configuration changes, through the date URE1 decommissioned the devices.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE1 did not have a systemic problem with configuration management. Due to human error, URE1 experienced an isolated occurrence of failure to follow its

[4] Possible Violations discovered during the CIP Compliance Audit will be addressed separately in the future.

documented change control and configuration management process. Although URE1 did not follow its change management process, it performed configuration testing at the time of the multiple software configuration changes to verify adequate and accurate data communication. The testing reduced the risk by validating that the devices were properly communicating to relays after the software configuration changes were implemented. The software configuration changes at issue were part of an engineering field package that required URE1 to perform multiple changes. URE1 performed the changes but did not follow its change control process when making the changes.

URE1's Mitigation Plan to address this violation was submitted to ReliabilityFirst stating that it had been completed. URE1's Mitigation Plan required URE1 to decommission the devices at issue.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-004-1 R2.1and R2.3 (RFC2012011471 and RFC2012010995)

During the Compliance Audit, ReliabilityFirst determined that URE4 and URE6 did not conduct CIP training for multiple individuals prior to granting the individuals physical access to Critical Cyber Assets (CCAs). In addition, URE4 did not perform annual CIP training for one individual.

ReliabilityFirst determined that URE4 and URE6 each had a violation of CIP-004-1 R2.1 and R2.3 because they did not conduct CIP training for multiple individuals prior to granting the individuals physical access to CCAs, and because they did not perform annual CIP training for one individual.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE4 and URE6, through the date URE4 and URE6 completed CIP training for the individuals at issue.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The individuals at issue received non-NERC cyber awareness training, which covered similar subject matter. URE4 and URE6 had conducted a personnel risk assessment (PRA) for the individuals at issue prior to granting the individuals physical access to CCAs. URE4 and URE6 discovered nothing in the PRAs that would have disqualified the individuals from being granted physical access to CCAs.

URE6's Mitigation Plan to address the violations of URE6 and URE4 was submitted to ReliabilityFirst stating it had been completed.

URE6's Mitigation Plan required URE6 to:

1. ensure individuals are trained when required;
2. accurately record training documentation; and
3. maintain sufficient records using its database.

URE6 certified on that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE6's Mitigation Plan was complete.

In addition, ReliabilityFirst determined the mitigating activities included in URE1's Mitigation Plan addressing prior violations of CIP-004-1 R1 and R2 sufficiently mitigate URE4's and URE6's instant violations of CIP-004-1 R2.1 and R2.3. URE1's Mitigation Plan laid out milestones to implement a database, which created an automated catalogue of user access to CCAs. This catalogue was integrated with other tracking systems to provide accurate dates related to training and PRAs. The instant violations of CIP-004-1 R2, before URE Parent Company incorporated the database into its practices at URE1, URE4, and URE6.

CIP-004-3 R4.2 (RFC2012010385 and RFC2012011443)

URE4 submitted a Self-Certification to ReliabilityFirst stating that it was in violation of CIP-004-3 R4. URE4 discovered that multiple non-URE Parent Company workers at a non-URE Parent Company facility that contained a URE4 physical security perimeter (PSP) did not have their physical access rights revoked within seven calendar days of those individuals' no longer requiring access to the PSP. URE4 determined that non-Unidentified Registered Entities' personnel were not consistently notifying URE4 when their personnel no longer required physical access to URE4's PSP.

URE3 submitted a Self-Report stating that it was in violation of CIP-004-3 R4.2. URE3 did not revoke physical access within seven calendar days for an administrative assistant who no longer required physical access.

ReliabilityFirst determined that URE4 and URE3 each had a violation of CIP-004-3 R4.3 because they did not revoke physical access to CCAs within seven calendar days for several individuals who no longer required physical access.

ReliabilityFirst determined the duration of the violation for URE4 to be from the date by which the workers should have had their physical access revoked, through the date their access was revoked.

The duration of the violation for URE3 was from the date URE3 should have revoked the administrative assistant's access, through the date access was revoked.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. None of the individuals at issue was terminated for cause, and none had logical access to URE Parent Company's CCAs. All individuals at issue had CIP training and PRAs at the time the violation occurred. Additionally, none of the individuals at issue accessed URE Parent Company's CCAs after it was determined that they no longer required access.

URE4's Mitigation Plan to address its violation of CIP-004-3 R4.2 was submitted to ReliabilityFirst stating it had been completed.

URE4's Mitigation Plan required URE4 to:

1. revoke access for the workers at issue; and
2. establish a process to notify URE4 when personnel with access to its PSP are transferred or no longer require PSP access.

URE4 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE4's Mitigation Plan was complete.

ReliabilityFirst determined that URE3's violation did not require a formal Mitigation Plan. URE3 revoked the access of the administrative assistant at issue. URE3 submitted evidence that it had revoked the access. ReliabilityFirst verified that URE3 completed the necessary mitigating activities.

CIP-005-3a R1.5 (RFC2012011272)

During the Compliance Audit, ReliabilityFirst determined that URE7 was using an administrator account on a checkpoint firewall that was not removed, disabled, or renamed as required by CIP-007-3 R5.2.1, referenced in CIP-005-3 R1.5. ReliabilityFirst determined that URE7 did not change the account name before the firewall went into service.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE7, through the date URE7 changed the password on the account.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, default account information on a firewall could leave

Unidentified Registered Entities' systems vulnerable to potential compromise. Default account information may be available in vendor publications, books, or on the internet and could be exploited by a malicious actor, thereby putting Unidentified Registered Entities' systems at a higher risk than those protected by non-default account information. The risk was mitigated by the fact that URE Parent Company employs a system of layered defenses. This defense-in-depth strategy provides additional layers of defense against unauthorized access and thereby mitigates the risk posed by the violation.

URE7's Mitigation Plan to address this violation was submitted to ReliabilityFirst stating it had been completed.

URE7's Mitigation Plan required URE7 to change the local default administrator account name for the checkpoint firewall.

In addition to the actions required by the Mitigation Plan, URE Parent Company affiliates, including URE7, combined their individual CIP programs into a single consolidated URE Parent Company CIP Program. As part of this consolidation, URE Parent Company developed more robust processes and procedures to ensure that accounts are removed, disabled, or renamed pursuant to CIP-007 R5.2.1 and CIP-005-3 R1.5. These processes and procedures included a change control and configuration management process that, among other things, ensures generic account names are changed before placing devices into service.

URE7 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE7's Mitigation Plan was complete.

CIP-005-3 R2.1 and R2.2 (RFC2012011061, RFC2012011067, RFC2012011123, and RFC2012011071)

URE4, URE5, and URE6 submitted Self-Reports to ReliabilityFirst stating that they were in violation of CIP-005-3 R2.1 and R2.2. URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of the same Reliability Standard and Requirements. URE4, URE5, URE6, and URE1 discovered that a network redesign (Redesign), which terminated some of their access control devices on a different cluster of firewalls, resulted in these devices not fully implementing the requirements of CIP-005-3 R2.1 and R2.2. Following the Redesign, the devices no longer denied access by default and did not independently restrict access to the associated ESP.

ReliabilityFirst determined that URE4, URE5, URE6, and URE1 had a violation of CIP-005-3 R2.1 and R2.2 because they did not enable their respective devices at issue to deny access by default and did not independently restrict access to the associated ESP.

ReliabilityFirst determined the duration of the violations to be from the date URE4, URE5, URE6 and URE1 performed the Redesign, through the date they configured the devices to deny all electronic communication transactions within the facility wide area network.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1, URE4, URE5, and URE6 had access control at the devices, access control via the upstream firewall, and access control to individual devices via server authentication. Furthermore, URE1, URE4, URE5, and URE6 had layered intrusion prevention defenses. These defenses included firewalls, intrusion detection and prevention defenses, malicious software prevention, and encryption, thereby limiting the risk from, and exposure to, external threats.

URE1, URE4, URE5, and URE6's Mitigation Plans to address these violations were submitted to ReliabilityFirst on stating they had been completed.

The Mitigation Plans required the entities to:

1. configure the access control lists on the devices to deny all electronic communication transactions within the facility network; and

2. configure the devices to restrict specific point access to the ESP and deny all other access to the ESP by default.

URE1, URE4, URE5, and URE6 certified that the above Mitigation Plans requirements were completed.

ReliabilityFirst verified that URE1, URE4, URE5, and URE6's Mitigation Plans were complete.

CIP-005-3a R3.2 (RFC2012011273)

During the Compliance Audit, ReliabilityFirst determined that URE7 was in violation of CIP-005-3a R3.2. URE7 did not adequately alert for access attempts or actual unauthorized access to its ESP. URE7 only alerted for failed login and local account creation for the duration of the violation.

ReliabilityFirst determined that URE7 had a violation of CIP-005-3a R3.2 because it did not implement a security monitoring process that detects and alerts for attempts at or actual unauthorized accesses.

ReliabilityFirst determined the duration of the violation to be from the date URE7 implemented a process which did not require URE7 to detect or alert for attempted or actual unauthorized access to its ESP, through the date URE7 revised its security monitoring process to detect and alert for attempted or actual unauthorized access to its ESP.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE7 continuously monitors and logs system events on the Cyber Assets within the ESP, as required by CIP-007 R6. URE7's firewalls were functioning properly by filtering and denying unauthorized access attempts to the ESP for the duration of the violation. URE7's firewalls were denying unauthorized access attempts to the ESP. URE7 did not receive alerts regarding unauthorized access attempts.

URE7’s Mitigation Plan to address this violation was submitted to ReliabilityFirst stating it had been completed.

URE7’s Mitigation Plan required URE7 to establish a security monitoring procedure that detects and alerts for access attempts to the ESP. The procedure requires logs of user account activity as required by CIP-007-3 R5.1.2.

URE7 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE7’s Mitigation Plan was complete.

CIP-005-1 R5.2 (RFC2012011062, RFC2012011068, RFC2012011072 and RFC2012011078)

URE1, URE4, URE5, and URE6 each submitted a Self-Report to ReliabilityFirst stating that they were in violation of CIP-005-1 R5. URE1, URE4, URE5, and URE6 discovered that each of them had failed to document changes to their ESP drawing resulting from the Redesign.

ReliabilityFirst determined that URE1, URE4, URE5, and URE6 each had a violation of CIP-005-1 R5.2 because they did not document within 90 days a modification that resulted in some of their respective devices terminating on a different cluster of firewalls.

ReliabilityFirst determined the duration of these violations to be from the date the entities should have documented the changes to the ESP, through the date the entities updated the ESP drawings to reflect the changes resulting from the Redesign.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The violations consisted of documentation errors. Specifically, although the drawings were not updated within 90 days to reflect the change to the network, appropriate URE Parent Company personnel prepared, approved, and implemented the changes. Further, all appropriate personnel were aware of the change because of the limited number of electronic access points and the fact that a small team of people maintains those assets.

URE1, URE4, URE5, and URE6's Mitigation Plans to address these violations were submitted to ReliabilityFirst, stating the four Mitigation Plans had been completed.

The Mitigation Plans required the entities to update their ESP drawings at issue to reflect the Redesign changes.

URE1, URE4, URE5, and URE6 certified that the above Mitigation Plans requirements were completed.

ReliabilityFirst verified that the Mitigation Plans were complete.

CIP-007-3a R1.1 (RFC2012010389)

URE1 submitted a Self-Certification to ReliabilityFirst stating that it was in violation of CIP-007-3a R1. URE1 determined that it prematurely installed an operating system security patch on multiple CCAs before the patch had been fully tested in accordance with URE1's cybersecurity test procedures. Specifically, URE1 determined that it had not tested the security patch in a CIP test environment to determine if the installation would result in any adverse effects to existing cybersecurity controls.

ReliabilityFirst determined that URE1 had a violation of CIP-007-3a R1.1 because it installed a system security patch on multiple CCAs before testing the patch.

ReliabilityFirst determined the duration of the violation to be from the date URE1 installed the security patch on the CCAs at issue, through the date URE1 tested the security patch in accordance with its cybersecurity test procedures.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The duration of the violation was short. URE1 quickly identified the issue and performed the required testing within a week. All patches were approved by third-party vendors. Additionally, upon testing the security patch in accordance with its cybersecurity test procedures, URE1 determined that the patch had no compatibility issues with the CCAs or their associated applications. The CCAs at issue were not needed or used for the duration of the violation. Therefore, the security patch had no adverse effects on the existing cybersecurity controls for the duration of the violation.

URE1 memorialized the actions it took to address this violation and no formal Mitigation Plan was required. URE1 tested the security patch at issue in accordance with its cybersecurity test procedures. Additionally, URE1 reconfigured software on applicable CIP workstations to ensure that patches are only available to those CIP workstations after IT real-time operations testers have tested and approved the security patches.

URE1 submitted evidence that it completed the mitigating activities.

ReliabilityFirst verified that URE1 completed the mitigating activities.

<u>CIP-007-1 R1.3 (RFC2012011063, RFC2012011069, RFC2012011073, and RFC2012011099)</u>

URE4, URE5, and URE6 each submitted a Self-Report stating that they were in violation of CIP-007-3 R1.3. URE1 submitted a Self-Report stating that it was in violation of CIP-007-1 R1.3. URE1, URE4, URE5, and URE6 discovered that they had not adequately documented the testing each entity performed on some of their devices to ensure these devices did not adversely affect existing cybersecurity controls.

ReliabilityFirst determined that URE1, URE4, URE5, and URE6 each had a violation of CIP-007-3 R1.3 because they did not document the test results for their devices.

ReliabilityFirst determined the duration of these violations to be from the date on which URE1, URE4, URE5, and URE6 were required to comply with this Standard, through the date they disconnected the dial-up connections and decommissioned the devices.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1, URE4, URE5, and URE6 performed testing required by CIP-007-1 R1 on the dial-up devices in accordance with URE Parent Company's approved test procedures; these violations represented documentation errors. Additionally, for the duration of the violations, URE1, URE4, URE5, and URE6 had implemented automated tools and organizational process controls to monitor events related to cybersecurity for remote access to the devices.

URE1, URE4, URE5, and URE6’s Mitigation to address these violations were submitted to ReliabilityFirst on stating they had been completed.

URE1, URE4, URE5, and URE6's Mitigation Plan required the entities to disconnect the dial-up connections and decommission the devices at issue.

URE1, URE4, URE5, and URE6 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the Mitigation Plans were complete.

CIP-007-1 R5 (RFC2012011101, RFC2012011064, RFC2012011074, and RFC2012011066)

URE1, URE4, URE5, and URE6 each submitted a Self-Report to ReliabilityFirst stating that they were in violation of CIP-007-1 R5. URE1, URE4, URE5, and URE6 discovered that they had not established, implemented, and documented technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access to a single local access port on some of their respective devices. URE1, URE4, URE5, and URE6 established, implemented, and documented remote access processes to ensure compliance with CIP-007-1 R5, but had not extended those processes to the local access port.

ReliabilityFirst determined that URE1, URE4, URE5, and URE6 each had a violation of CIP-007-1 R5 because they did not establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all local logical access to dial-up devices.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE1, URE4, URE5, and URE6, through the date they disconnected dial-up connections and decommissioned the devices at issue.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Unauthorized access to the local service port on the devices would require physical access through a locked fence and a locked building door, which is monitored for entry by URE Parent Company. Access via the local service port is password-protected, and an alarm is generated the event of unauthorized access attempts to the devices. Finally, for remote access to the devices at issue, URE1, URE4, URE5, and URE6 implemented automated tools and organizational process controls to monitor system events that are related to cybersecurity.

URE1, URE4, URE5, and URE6's Mitigation Plans to address these violations were submitted to ReliabilityFirst, stating the Mitigation Plans had been completed.

URE1, URE4, URE5, and URE6's Mitigation Plans required them to disconnect dial-up connections and decommission the devices at issue.

URE1, URE4, URE5, and URE6 certified that the above Mitigation Plan requirements were complete.

ReliabilityFirst verified that URE1, URE4, URE5, and URE6's Mitigation Plans were complete.

CIP-007-1 R5.3.3 (RFC2012010386)

On May 2, 2012, URE2 submitted a Self-Certification stating that it was in violation of CIP-007-1 R5.3.3. During its Cyber Vulnerability Assessment, URE2 determined that it did not annually change passwords for multiple local accounts at one Critical Asset facility, and that it did not delete these accounts when it installed an active directory to manage passwords. Additionally, URE2 determined it did not establish log-on passwords for the shared operator account on several devices at the same facility.

ReliabilityFirst determined that URE2 had a violation of CIP-007-1 R5.3.3 for a failure to change passwords annually for one Critical Asset facility.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE2, through the date URE2 decommissioned the applicable Critical Asset.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The devices at issue were located within a PSP. URE2 employs a system of layered defenses. This defense-in-depth strategy provides additional layers of defense against unauthorized access and reduces the risk posed by this violation.

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

URE2's Mitigation Plan required URE2 to disable the local accounts and to decommission the Cyber Assets at issue.

URE2 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE2's Mitigation Plan was complete.

CIP-007-3a R5.3.3 (RFC2012011077)

URE7 submitted a Self-Report stating that it was in violation of CIP-007-3a R5.3.3. URE7 discovered that it had not updated passwords for multiple individual user accounts and several shared system accounts annually. Prior to the discovery of this violation, the CCAs at issues were migrated from a legacy CIP program to a new URE Parent Company CIP program, which included affiliated companies. Because of the consolidation of programs, the timing of the controls occurred such that annual password changes for the passwords at issue occurred more than 15 months apart when these password changes were synchronized with the combined URE Parent Company CIP program.

ReliabilityFirst determined that URE7 had a violation of CIP-007-3a R5.3.3 for its failure to change passwords annually for several accounts.

ReliabilityFirst determined the duration of the violation to be from the date by which URE7 should have updated its passwords, through the date URE7 updated the passwords at issue.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The duration of the violation was approximately one month. Furthermore, the passwords addressed the complexity requirements of CIP-007-3a R.5.3.1 and R5.3.2. Finally, the passwords at issue were available to authorized users only.

ReliabilityFirst determined that a formal Mitigation Plan was not required for this violation. In its Self-Report, URE7 represented that it completed all necessary mitigating actions to address this violation. URE7 changed all passwords at issue. Further, URE Parent Company's CIP program, which URE7 now follows, requires that the dates of the last password change be reviewed every six months, thus reducing the likelihood of missing an annual update.

URE7 submitted evidence that it completed these mitigating activities. ReliabilityFirst verified completion of these mitigating activities.

CIP-007-1 R6 (RFC2012011102, RFC2012011065, RFC2012011070, and RFC2012011075)

URE1, URE4, URE5, and URE6 each submitted a Self-Report stating that each was in violation of CIP-007-1 R6. URE1, URE4, URE5, and URE6 discovered that they had not adequately monitored local logical access to some devices for system events that are related to cybersecurity.

ReliabilityFirst determined that URE1, URE4, URE5 and URE6 each had a violation of CIP-007-1 R6 for a failure to monitor system events related to cybersecurity of some of their devices.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE1, URE4, URE5, and URE6, through the date the entities disconnected the dial-up connections and decommissioned the devices.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Unauthorized access to the local service port on the devices would require physical access through a locked fence and a locked door which is monitored for entry. Access via the local service port is password-protected, and an alarm is generated in the URE Parent Company in the event of unauthorized access attempts the devices. Finally, for remote access to the devices, URE1, URE4, URE5, and URE6 implemented automated tools and organizational process controls to monitor system events that are related to cybersecurity.

URE1, URE4, URE5, and URE6’s Mitigation Plans to address these violations were submitted to ReliabilityFirst stating they had been completed.

URE1, URE4, URE5, and URE6’s Mitigation Plans required these entities to disconnect dial-up connections and decommission the dial-up devices at issue.

URE1, URE4, URE5, and URE6 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the URE1, URE4, URE5, and URE6 Mitigation Plans were complete.

CIP-007-1 R6 (RFC2012010387)

URE2 submitted a Self-Certification stating that it was in violation of CIP-007-1 R6. URE2 discovered that it had not adequately implemented organizational processes and technical and procedural mechanisms for monitoring security events for several CCAs. URE2 discovered this violation after it decommissioned the CCAs at issue.

ReliabilityFirst determined that URE2 had a violation of CIP-007-1 R6 for failing to implement adequately organizational processes and technical and procedural mechanisms for monitoring security events on several CCAs.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE2, through the date URE2 decommissioned the CCAs at issue.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, use of the network switches by a malicious actor could result in the loss of operational control or visibility. Further, without security controls and monitoring in place, the malicious actor could remain undetected. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. These CCAs were enclosed in PSPs during the violation period, and physical access was controlled and monitored in accordance with the CIP Standards. Further, during the violation period, access points to the ESPs and other CIP Cyber Assets in the ESPs were monitored, and logging was performed as required by the CIP Standards.

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

URE2's Mitigation Plan required URE2 to decommission the CCAs at issue.

URE2 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE2's Mitigation Plan was complete.

CIP-007-3a R7.3 (RFC2012011076)

URE6 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-007-3 R7.3. When one URE6 device failed in service, URE6 sent the device for repair. Upon receipt of the repaired device, URE6 designated the device as a spare device and placed it in storage. URE6 did not properly maintain records associated with the redeployment of the device. Upon decommissioning of the device, URE6 discovered that it did not maintain redeployment records after it removed the device from service for repair.

ReliabilityFirst determined that URE6 had a violation of CIP-007-3 R7.3 for its failure to maintain records that it redeployed one device in accordance with its documented procedures.

ReliabilityFirst determined the duration of the violation to be from the date URE6 redeployed the single device as a spare device, through the date URE6 disconnected dial-up connections and decommissioned the device.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. ReliabilityFirst determined that this violation involved a documentation issue because URE6 redeployed the device pursuant to CIP-007 R7, but it did not maintain the associated records adequately.

URE6's Mitigation Plan to address this violation was submitted to ReliabilityFirst, stating that it had been completed.

URE6's Mitigation Plan required URE6 to disconnect the dial-up connections and decommission the device at issue.

URE6 certified that the above Mitigation Plan requirements were completed.

On August 5, 2013, ReliabilityFirst verified that URE6's Mitigation Plan was complete.

CIP-009-1 R1 (RFC2012011265, RFC2012011268, and RFC2012011270)

During the Compliance Audit, ReliabilityFirst determined that URE4, URE5, and URE6 did not have an adequate recovery plan for some of their respective devices. URE4, URE5, and URE6 had procedures to address recovery of the devices at issue. However, these procedures did not address all the elements required by CIP-009-1 R1. The applicable procedures did not specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan and did not define the roles and responsibilities of responders.

ReliabilityFirst determined that URE4, URE5, and URE6 each had a violation of CIP-009-3 R1 because they did not have adequate recovery plans for their respective devices.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE4, URE5, and URE6, through the date the entities disconnected the dial-up connections and decommissioned the devices.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The recovery plans identified other procedures that were invoked by the loss of a communication processor and the overall steps to address repair or replacement of the devices in the event of a communication processor failure. In addition, the recovery plan did identify the responders, although it did not adequately define the roles and responsibilities of those responders. Further, the violation did not indicate a systemic issue with URE4, URE5, and URE6's respective recovery plans. During the Compliance Audit, ReliabilityFirst determined these Unidentified Registered Entities had recovery plans for all devices except the devices.

URE4, URE5, and URE6's Mitigation Plans to address these violations were submitted to ReliabilityFirst stating they had been completed.

URE4, URE5, and URE6's Mitigation Plans required the entities to disconnect the dial-up connections and decommission the devices.

URE4, URE5, and URE6 certified on that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE4, URE5, and URE6's Mitigation Plans were complete.

Internal Control Improvements

ReliabilityFirst determined that the Unidentified Registered Entities have implemented programs and procedures that substantially improve their shared compliance program by optimizing the Unidentified Registered Entities' operations and security. Many of these improvements began as part of an effort to consolidate the Unidentified Registered Entities' separate compliance programs into a single compliance program. Many of the instant violations were corrected in the scope of the Unidentified Registered Entities' efforts, and therefore represent historical compliance issues. Unidentified Registered Entities' efforts to improve compliance had affected five major compliance areas: 1) change control and configuration management; 2) cybersecurity logging; 3) identifying and classifying Cyber Assets; 4) access control and account management; and 5) testing.

Thus, ReliabilityFirst determined that the internal controls improvements outlined above, which can be tied to the key management practices of asset and configuration management and reliability quality management, have positioned URE Parent Company to be more reliable and compliant on a going-forward basis.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of fifty thousand dollars ($50,000) for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors:

1. the violations constituted Unidentified Registered Entities' fifth occurrence of same or similar violations of CIP-004 and second occurrence of same or similar violations of CIP-007. ReliabilityFirst considered the compliance history of the Unidentified Registered Entities as an aggravating factor in the penalty determination, but not a substantial aggravating factor;
2. the subsequent CIP Compliance Audit findings (to be addressed separately in the future) demonstrated the Unidentified Registered Entities' maturing compliance program through its efforts to improve internal controls;
3. ReliabilityFirst awarded significant mitigating credit to recognize and incent the Unidentified Registered Entities' substantial and voluntary commitment to improve its operations and compliance program. ReliabilityFirst favorably considered the Unidentified Registered Entities' efforts, which ReliabilityFirst observed firsthand during the Compliance Audit, at improving CIP compliance and enhancing the reliability of the BPS;
4. ReliabilityFirst favorably considered certain aspects of the Unidentified Registered Entities' compliance programs. ReliabilityFirst also favorably considered the various improvements to URE Parent Company's compliance program and internal controls, which largely began prior to the Compliance Audit and address legacy issues that led to findings of noncompliance at the Compliance Audit;
5. the Unidentified Registered Entities self-reported 24 of the violations;[5]
6. of the total 35 violations, 33 violations posed minimal risk to the reliability of the BPS, as discussed above. The violations did not indicate systemic failure, and were promptly mitigated;
7. two of the 35 violations posed a moderate risk to the reliability of the BPS, as discussed above;
8. the Unidentified Registered Entities were cooperative throughout the compliance enforcement process;
9. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so; and
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[5] ReliabilityFirst applied partial mitigating credit for 21 of the 24 Self-Reports and full mitigating credit for the remaining three Self-Reports.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of fifty thousand dollars ($50,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[6]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on July 15, 2014. The NERC BOTCC approved the Settlement Agreement, including ReliabilityFirst's assessment of a fifty-thousand dollar ($50,000) financial penalty against the Unidentified Registered Entities 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 also considered the factors considered by ReliabilityFirst, as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of fifty thousand dollars ($50,000) 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.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

[6] *See* 18 C.F.R. § 39.7(d)(4).

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

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 Niki Schaefer* Managing Enforcement Attorney ReliabilityFirst Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542 (216) 503-0689 (216) 503-9207 – facsimile niki.schaefer@rfirst.org	Sonia C. Mendonça* Associate 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 Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net
L. Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542 (216) 503-0683	Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542

(216) 503-9207 – 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.	(216) 503-0682 (216) 503-9207 – facsimile bob.wargo@rfirst.org

Conclusion

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

Respectfully submitted,

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

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

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

Sonia C. Mendonça
Associate 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

cc: Unidentified Registered Entities
ReliabilityFirst Corporation

Attachments