October 30, 2013

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

Re: NERC Full Notice of Penalty regarding URE
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 (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 ReliabilityFirst Corporation (RF) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from RF's determination and findings of the violations[3] of CIP-004-1 R2, R3.3, and R4, CIP-007-3 R1, R3 and R5. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of zero dollars ($0), 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 RFC201000288, RFC201000289, RFC201000290, RFC2012010329, RFC2012010349, RFC2012011205, and RFC2012010350 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

---

[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).

[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.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on August 5, 2013, by and between RF 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
ReliabilityFirst Corporation	URE	NOC-2178	RFC201000288	CIP-004-1	R2	Lower	$0
			RFC201000289	CIP-004-1	R3; R3.3	Lower	
			RFC201000290	CIP-004-1	R4	Lower	
			RFC2012010329	CIP-004-3	R4	Lower	
			RFC2012010349	CIP-007-3a	R1; R1.1	Moderate	
			RFC2012011205	CIP-007-3	R3; R3.1	Lower	
			RFC2012010350	CIP-007-3a	R5; R5.2.2; R5.3.3	Lower	

CIP-004-1

The purpose statement of Reliability Standard CIP-004-1 in pertinent part provides: "that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and

security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-004-1 R2 provides in pertinent part:

> R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
>
> R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.
>
> R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:
>
> R2.2.1. The proper use of Critical Cyber Assets;
>
> R2.2.2. Physical and electronic access controls to Critical Cyber Assets;
>
> R2.2.3. The proper handling of Critical Cyber Asset information; and,
>
> R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.
>
> R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records

CIP-004-1 R2 has a "Lower" Violation Risk Factor (VRF) and a "Lower" Violation Severity Level (VSL).

CIP-004-1 R3 provides in pertinent part:

> R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel

having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

***

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

CIP-004-1 R3.3 has a "Lower" VRF and a "Lower" VSL.

CIP-004-1 R4 provides in pertinent part:

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. the Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-004-1 R4 has a "Lower" VRF and a "Lower" VSL.

CIP-004-1 R2

During a Spot Check RF determined that URE was in violation of CIP-004-1 R2. URE failed to present adequate evidence of documentation demonstrating that all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) were trained within 90 calendar days of URE granting such access. URE also failed to maintain documentation establishing that URE conducts training at least annually for all personnel having authorized cyber or authorized unescorted

physical access to CCAs. Specifically, URE failed to demonstrate that URE gave cybersecurity training to one contractor within 90 calendar days of granting the individual access to CCAs. Additionally, URE did not provide training dates for 10 individuals with access to CCAs and did not provide adequate training records for five of these 10 individuals. Finally, URE did not have sufficient evidence of annual cybersecurity training for one contractor.

RF determined the duration of the violation to be from the date when the Standard became mandatory and enforceable on URE through when URE completed its mitigating activities.

RF determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). RF determined this violation posed a minimal risk because URE performed training for all the individuals impacted in this violation, but it failed to retain documentation of the training. Additionally, at all relevant times, URE maintained a requirement that individuals receive cybersecurity training.

CIP-004-1 R3.3
During a Spot Check RF determined that URE was in violation of CIP-004-1 R3.3. URE failed to maintain documentation of the results of personnel risk assessments (PRAs) for its personnel having access to CCAs. Specifically, URE could not provide result records of the PRAs for 18 individuals having authorized cyber or authorized unescorted physical access to CCAs.

RF determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its mitigating activities.

RF determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE performed the PRAs for the affected individuals and tracked these PRAs in a spreadsheet. Additionally, URE was able to provide some payment invoices during the Spot Check to support its performance of PRAs, although it was unable to produce the original copies of the PRAs. URE had not retained this evidence prior to the transition to mandatory Reliability Standards. Following the Spot Check, URE again performed PRAs for all those employees for whom URE could not locate actual vendor certified PRAs and discovered no adverse results.

CIP-004-1 R4
During a Spot Check RF determined that URE was in violation of CIP-004-1 R4. URE failed to maintain the access lists of personnel with authorized cyber or authorized unescorted physical access rights to CCAs, including their specific electronic and physical access rights to CCAs. RF reviewed the access list

showing access permission and the list of personnel granting access permission. These lists contained discrepancies, indicating URE's failure to maintain the access lists of personnel with access to CCAs.

RF determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE required that all individuals, regardless of access type, submit to regular PRAs and complete the security training on an annual basis. The PRAs ensured that URE personnel did not have problematic backgrounds. The cybersecurity training included password security training. In addition, URE conducted a quarterly recertification and reconciliation of the authorized user list. The recertification ensured that URE's authorized list was maintained accurately, and the reconciliation ensured that the provisioned access matches URE's list of authorized users. The account authorization team performed daily reconciliations of changes in logical access to CCAs to ensure that access is implemented as authorized. The platform operations group at URE implemented a peer review process to help ensure that access was provisioned appropriately. Furthermore, URE monitors important physical access points with security guards, video surveillance, or both at all relevant times.

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

CIP-004-3

The purpose statement of Reliability Standard CIP-004-3 provides in pertinent part: "Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness."

CIP-004-3 R4 provides in pertinent part:

> R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
>
> > R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

> R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-004-3 R4 has a "Lower" VRF and a "Lower" VSL.

URE submitted a Self-Report stating that it was in violation of CIP-004-3 R4. During a quarterly review of its access lists, URE noted instances in which it did not properly maintain lists of personnel with authorized cyber access to CCAs. Specifically, URE identified eight instances in which it did not properly maintain lists of personnel with access to CCAs.

RF determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE required that all individuals, regardless of access type, submit to regular PRAs and complete the security training on an annual basis. The PRAs ensured that URE personnel did not have problematic backgrounds, and the cybersecurity training included password security training. In addition, URE conducted a quarterly recertification and reconciliation of the authorized list. The recertification ensured that URE's authorized list was maintained accurately, and the reconciliation ensured that the provisioned access matches URE's list of authorized users. The URE implemented a peer review process to help ensure that access was provisioned appropriately. Furthermore, URE monitors important physical access points by security guards, video surveillance, or both at all relevant times.

RF determined the duration of the violation to be from the date URE did not properly maintain lists of personnel with authorized access to CCAs, through when URE completed its Mitigation Plan.

CIP-007-3a

The purpose statement of Reliability Standard CIP-007-3a 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-007-3a 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-007-3, 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-007-3a R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it was in violation of CIP-007-3a R1. URE failed to ensure that significant changes to existing Cyber Assets within the Electronic Security Perimeter (ESP) did not adversely affect existing cybersecurity controls. First, URE did not conduct testing procedures prior to deploying a software product, which constituted a significant change, on a Cyber Asset within the ESP. Therefore, URE could not ensure that the significant change to the Cyber Asset within the ESP did not adversely affect existing cybersecurity controls. Second, URE did not conduct testing procedures prior to implementing a security patch, which constituted a significant change, on a Cyber Asset within the ESP. Therefore, URE could not ensure that the significant change to the Cyber Asset within the ESP did not adversely affect existing cybersecurity controls.

RF determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. For the software product, URE validated, approved, deployed, and operated the software product in its non-CIP IT infrastructure prior to extending the functionality into the CIP ESP networks. Moreover, URE's subsequent testing validated that installation of the software had no adverse effect on the cybersecurity controls of the CIP Critical Assets where the software was installed. The Cyber Assets on which the software was deployed were protected according to all CIP standards. URE had several monitoring processes in place that would have alerted it of any changes to security controls. These controls help in identifying any potential impact to the Cyber Assets in the ESP.

In terms of the security patch, the patch superseded a previous security patch to address vulnerabilities in a URE system. URE tested the previous security patch according its defined test procedures. As a result, the new security patch that was deployed to a subset of Cyber Assets in the ESP had been partially tested. The new security patch eliminated additional vulnerabilities that were identified for a component of the system. The patch resolved vulnerabilities that would not necessarily be perceived as high risk. URE's intrusion detection system and cybersecurity event monitoring system also monitor for any malicious activity directed at ESPs. These controls help in identifying any potential impact to the Cyber Assets in the ESP.

RF determined the duration of the violation to be from the date URE implemented a significant change to existing Cyber Assets within the ESP without first ensuring that the change did not adversely affect existing cyber security controls, through when URE completed its Mitigation Plan.

CIP-007-3a 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.
>
> ***
>
> R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.
>
> ***
>
> R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:
>
> ***
>
> R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

CIP-007-3a R5 has a "Lower" VRF and a "Severe" VSL.

URE submitted Self-Reports stating that it was in violation of CIP-007-3 R5. URE self-reported two instances where individuals were able to access shared accounts, but URE had not previously identified these individuals as having access to shared accounts, as required by CIP-007-3 R5.2.2. Additionally, URE identified a violation of CIP-007-3 R5.3.3 for failing to change annually the password to an account.

RF determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. RF determined this violation posed a moderate risk because in the first instance in which individuals were able to access shared accounts, the URE personnel noted as using the shared account password had access to the shared account appropriately and, therefore, should have appeared on URE's list of users with authorized access to the shared accounts in question. In terms of the second instance in which an individual was able to access a shared account, the password utilized by the unauthorized individual granted equivalent access to the CCAs as the access that would have been granted to that same individual through the application of the individual's personal identification and password. Additionally, URE required that all individuals, regardless of access type, submit to regular PRAs and complete the security training on an annual basis. The PRAs ensured that URE personnel did not have problematic backgrounds, and the security training included statements concerning the need for security of passwords.

In terms of URE's failure to change a database password annually, URE provided other safeguards to ensure the protection of Cyber Assets within the ESPs were in place and functioning properly. URE installed the database within an ESP, which provided network-based security controls to limit access. Furthermore, the database enforces password standards to ensure that passwords are strongly constructed. The database also implements audit logging for centralized review at least weekly, and URE performs an annual cyber vulnerability assessment for the device. Finally, URE reviewed accounts at least annually to ensure that all accounts are authorized.

RF determined the duration of the violation to be from the date of URE's missed annual password change, through when URE completed its Mitigation Plan.

CIP-007-1

The purpose statement of Reliability Standard CIP-007-1 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-007-1 R3 provides in pertinent part:

> R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber

security software patches for all Cyber Assets within the 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.

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

URE submitted a Self-Report stating that it was in violation of CIP-007-1 R3. URE self-reported that it failed to complete a documented assessment within 30 calendar days of availability for three security patches.

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. URE reported that there have been no instances affecting the availability of the Cyber Assets.

RF determined the duration of the violation to be the date by which URE should have documented an assessment of the first security patch associated with this violation, through when URE completed its Mitigation Plan.

Regional Entity's Basis for Penalty

RF assessed a penalty of zero dollars ($0) for the referenced violations. In reaching this determination, RF considered the following factors:

1) URE's compliance history, which was not considered an aggravating factor;
2) URE self-reported several of the violations, as discussed herein, which RF considered a mitigating factor;
3) URE had an internal compliance program (ICP) at the time of the violations, which RF considered a mitigating factor;
4) URE was cooperative throughout the compliance enforcement process;
5) The violations posed a minimal or moderate risk, as discussed herein, to the reliability of the BPS and did not pose a serious or substantial risk to the BPS;
6) there was no evidence of any attempt by URE to conceal the violation;
7) there was no evidence that URE's violations were intentional;
8) URE performed above and beyond actions to enhance the reliability of the BPS; and
9) there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

Status of Mitigation Plan[4]

RFC201000288 (CIP-004-1 R2)
URE's mitigating activities to address its violation of CIP-004-1 R2 were submitted to RF.

URE's mitigating activities required URE to:

1. disable each individual's access;
2. require the individuals to complete cybersecurity training;
3. take additional steps to ensure retention of training records;
4. eliminate the signed paper; and
5. formalize the process.

URE certified that the above mitigating activities requirements were completed. URE submitted evidence of completion of its mitigating activities to RF.

After RF's review of URE's submitted evidence, RF verified that URE's mitigating activities were completed.

RFC201000289 (CIP-004-1 R3.3)
URE's mitigating activities to address its violation of CIP-004-1 R3.3 was submitted to RF.

URE's mitigating activities required URE to perform PRAs for all those employees for whom URE could not locate actual vendor-certified PRAs.

URE certified that the above mitigating activities requirements were completed. URE submitted evidence of completion of its mitigating activities to RF.

After RF's review of URE's submitted evidence, RF verified that URE's activities were completed.

RFC201000290 (CIP-004-1 R4) and RFC2012010329 (CIP-004-3 R4)
URE's Mitigation Plan to address its violations of CIP-004-1 R4 and CIP-004-3 R3 was submitted to RF. The Mitigation Plan was accepted by RF and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007479 and was submitted as non-public information to FERC.

[4] *See* 18 C.F.R § 39.7(d)(7).

URE's Mitigation Plan required URE to:

1. remediate the specific instances in which it did not properly maintain access lists by either removing the access or updating records to ensure URE's list of authorized users accurately reflected the actual access provisioned on systems;
2. initiate a daily account reconciliation process;
3. conduct a peer review of the reconciliation to ensure all unauthorized accounts have been identified;
4. conduct training; and
5. remind URE personnel of the importance of CIP-004 R4 compliance.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of completion of its Mitigation Plan to RF.

After RF's review of URE's submitted evidence, RF verified that URE's Mitigation Plan was completed.

RFC2012010349 (CIP-007-3a R1)

URE's Mitigation Plan to address its violation of CIP-007-3a R1.1 was submitted to RF. The Mitigation Plan was accepted by RF and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007478 and was submitted as non-public information to FERC.

URE's Mitigation Plan required URE to:

1. complete the cybersecurity test procedures for the product and establish, document, and implement procedural controls for deploying new versions of the product;
2. require each patch management team member to attest to the reading and understanding of URE's Procedure;
3. modify URE's change management documentation requirement for patch deployment to Cyber Assets; and
4. train relevant staff on the modification to URE's procedure.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of completion of its Mitigation Plan to RF.

After RF's review of URE's submitted evidence, RF verified that URE's Mitigation Plan was completed.

RFC2012011205 (CIP-007-1 R3)

URE's Mitigation Plan to address its violation of CIP-007-3 R3.1 was submitted to RF. The Mitigation Plan was accepted by RF on and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008532 and was submitted as non-public information to FERC.

URE's Mitigation Plan required URE to:

1. complete a documented assessment of the patches for applicability;
2. register to receive patch notifications from the patch vendors;
3. install applicable patches; and
4. conduct a review to verify no other patches were released, but not assessed.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of completion of its Mitigation Plan to RF.

RFC2012010350 (CIP-007-3a R5)

URE's Mitigation Plan to address its violation of CIP-007-3a R5 was submitted to RF. The Mitigation Plan was accepted by RF and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007481 and was submitted as non-public information to FERC.

URE's Mitigation Plan required URE to:

1. remediate the two involved accounts;
2. review password security with relevant personnel;
3. update documentation of shared accounts to ensure clarity of process and policy;
4. publish a message to remind personnel of password security; and
5. change the password for its database account and create a checklist to ensure that URE personnel follow consistent procedures for changing the database password in the future.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of completion of its Mitigation Plan to RF.

After RF's review of URE's submitted evidence, RF verified that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[5]

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,[6] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on October 8, 2013. The NERC BOTCC approved the Settlement Agreement, including RF's assessment of a zero dollar ($0) 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 self-reported some of the violations;
2. RF reported that URE was cooperative throughout the compliance enforcement process;
3. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
4. RF determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
5. Above and Beyond measures URE implemented to mitigate the violations, as described above; and
6. RF 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 zero dollars ($0) 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.

[5] *See* 18 C.F.R. § 39.7(d)(4).
[6] *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).

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 RF and URE, included as Attachment a;
b) Record documents for the violation for CIP-004-1 R2, included as attachment b:
    a. RF's Procedural Summary for Possible Violations for CIP-004-1 R2.1, included as Attachment b-1;
    b. RF's Procedural Summary for Possible Violations for CIP-004-1 R2.3, included as Attachment b-2;
    c. RF's Verification of Mitigation Plan Actions for CIP-004-1 R2, included as Attachment b-3; and
c) Record documents for the violation of CIP-004-1 R3, included as attachment c:
    a. RF's Procedural Summary for Possible Violations for CIP-004-1 R3.3, included as Attachment c-1;
    b. Verification of Mitigation Plan Actions for CIP-004-1 R3, included as attachment c-2.
d) Record documents for the violation of CIP-004-1 R4, included as attachment d
    a. RF's Procedural Summary for Possible Violations for CIP-004-1 R4, included as Attachment d-1;

b. URE's Mitigation Plan designated as RFCMIT007479 for CIP-004-3 R4, included as Attachment d-2.
c. URE's Certification of Mitigation Plan Completion for RFCMIT007479, included as Attachment d-3; and
d. Verification of Mitigation Plan Completion for RFCMIT007479, included as attachment e-4.

e) Record documents for the violation of CIP-004-3 R4, included as attachment e:
   a. URE's Self-Report for CIP-004-3 R4, included as Attachment e-1;
   b. URE's Mitigation Plan designated as RFCMIT007479 for CIP-004-3 R4, included as Attachment e-2;
   c. URE's Certification of Mitigation Plan Completion for CIP-004-3 R4, included as Attachment e-3; and
   d. Verification of Mitigation Plan Completion for CIP-004-3 R4, included as attachment e-4.
f) Record documents for the violation of CIP-007-3a R1, included as attachment f:
   a. URE's Self-Report for CIP-007-3 R1.1, included as Attachment f-1;
   b. URE's Mitigation Plan designated as RFCMIT007480 for CIP-007-3 R1, included as Attachment f-2;
   c. URE's Certification of Mitigation Plan Completion for CIP-007-3 R1, included as Attachment f-3.
   d. Verification of Mitigation Plan Completion for CIP-007-3 R1, included as attachment f-4.
g) Record documents for the violation of CIP-007-3 R3, included as attachment g:
   a. URE's Self-Report for CIP-007-1 R3.1, included as Attachment g-1;
   b. URE's Self-Report for CIP-007-3a R3.1, included as Attachment g-2;
   c. URE's Mitigation Plan designated as RFCMIT008532 for CIP-007-1 R3, included as Attachment g-3; and
   d. URE's Certification of Mitigation Plan Completion for CIP-007-1 R3, included as Attachment g-4.
h) Record documents for the violation of CIP-007-3 R3, included as attachment h:
   a. URE's Self-Report for CIP-007-3 R5.3.3, included as Attachment h-1;
   b. URE's Self-Report for CIP-007-3 R5.2.2 , included as Attachment h-2;
   c. URE's Mitigation Plan designated as RFCMIT007481 for CIP-007-3 R5, included as Attachment h-3;
   d. URE's Certification of Mitigation Plan Completion for CIP-007-3 R5 included as Attachment h-4; and
   e. Verification of Mitigation Plan Completion for CIP-007-3 R5, included as attachment h-5.

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
ReliabilityFirst 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
ReliabilityFirst 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 of 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
ReliabilityFirst 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 of Enforcement Processing
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: URE
ReliabilityFirst Corporation

Attachments