PRIVILEGED AND CONFIDENTIAL INFORMATION HAVE BEEN REMOVED FROM THIS PUBLIC VERSION

March 27, 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 Unidentified Registered Entity 1, Unidentified Registered Entity 2, and Unidentified Registered Entity 3,
FERC Docket No. NP13-_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), NERC Registry ID# NCRXXXXX, Unidentified Registered Entity 2 (URE2), NERC Registry ID# NCRXXXXX, and Unidentified Registered Entity 3 (URE3), NERC Registry ID# NCRXXXXX, (collectively, the UREs), 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 the UREs 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-004-1 R2; CIP-005-1 R1, R2, R4 and R5; CIP-006-1 R1; and CIP-007-1 R3, R5 and R9. According to the Settlement Agreement, the UREs admit that the facts stipulated constitute violations, and have agreed to the assessed penalty of one hundred twenty thousand dollars ($120,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and

[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.

conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers RFC2011001148, RFC2011001157, RFC2011001149, RFC2011001158, RFC2011001166, RFC2011001150, RFC2011001159, RFC2011001167, RFC2011001160, RFC2011001152, RFC2011001161, RFC2011001169, RFC2011001153, RFC2011001162, RFC2011001170, RFC2011001154, RFC2011001163, RFC2011001171, RFC2011001155, RFC2011001164, RFC2011001172, RFC2011001156, RFC2011001165, and RFC2011001173 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 on August 22, 2012, by and between Reliability*First* and the UREs, which is included as Attachment a. 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	URE1	NOC-1628	RFC2011001148	CIP-004-1	R2	Medium	$120,000
	URE2		RFC2011001157				
	URE1		RFC2011001149	CIP-005-1	R1	Medium	
	URE2		RFC2011001158				
	URE3		RFC2011001166				
	URE1		RFC2011001150	CIP-005-1	R2	Medium	
	URE2		RFC2011001159				
	URE3		RFC2011001167				

	URE2		RFC2011001160	CIP-005-1	R4	Medium	
	URE1		RFC2011001152	CIP-005-1	R5	Lower	
	URE2		RFC2011001161				
	URE3		RFC2011001169				
	URE1		RFC2011001153	CIP-006-1	R1	Medium	
	URE2		RFC2011001162				
	URE3		RFC2011001170				
	URE1		RFC2011001154	CIP-007-1	R3	Lower	
	URE2		RFC2011001163				
	URE3		RFC2011001171				
	URE1		RFC2011001155	CIP-007-1	R5	Medium	
	URE2		RFC2011001164				
	URE3		RFC2011001172				
	URE1		RFC2011001156	CIP-007-1	R9	Lower	
	URE2		RFC2011001165				
	URE3		RFC2011001173				

ReliabilityFirst and Midwest Reliability Organization (MRO) conducted a Compliance Audit of the UREs. The UREs operate from the same control room and share the same energy management system.

CIP-004-1 R2 (RFC2011001148 and RFC2011001157)

The purpose statement of Reliability Standard CIP-004-1 provides, in pertinent part: "Standard CIP-004 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-004-1 R2 provides:

> R2. Training — The Responsible Entity[4] 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.

[4] Within the text of Standard CIP-004, CIP-005, CIP-006 and CIP-007, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

> 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.

[Footnote added.]

CIP-004-1 R2 has a "Medium" Violation Risk Factor (VRF)[5] and a "High" Violation Severity Level (VSL).[6]

During the Compliance Audit, Reliability*First* and MRO discovered that certain personnel from a third-party entity had authorized cyber and authorized unescorted physical access to URE1 and URE2's Critical Cyber Assets (CCAs). The training program utilized by this third-party entity did not contain: (a) the proper use of CCAs, as required by CIP-004-1 R2.2.1 and (b) action plans and procedures to recover or re-establish CCAs and access thereto following a Cyber Security Incident, as required by R2.2.4.

Reliability*First* determined that URE1 and URE2 had violations of CIP-004-1 R2 because they failed to implement a cybersecurity training program for personnel with authorized cyber or authorized unescorted physical access to CCAs.

Reliability*First* determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE1 and URE2 through when URE1 and URE2 completed their Mitigation Plans.

Reliability*First* determined that these violations posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. The violations posed a moderate risk because they increase the likelihood that untrained personnel may have cyber or unescorted physical access to CCAs. This access could result in harm to the integrity of the CCA or the reliability of the BPS as a result of the untrained individuals' actions. However, the risk was mitigated by the fact that the third-party entity at issue did conduct cybersecurity training with the employees at issue, although that training did not meet all of the requirements under the Standard. Further, the majority of individuals with access to URE1 and URE2's CCAs were URE1 and URE2 employees, all of whom had received the required training and personnel risk assessments.

---

[5] The VRF for CIP-004-1 R2 is "Lower." However, the UREs' violations involved R2.2, which has a "Medium" VRF. Additionally, CIP-004-1 R2.2.1, R2.2.2 and R2.2.3 have a "Lower" VRF, while R2.2.4 has a "Medium" VRF.

[6] On the start date of the violations, no VSLs were in effect for CIP-004-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

CIP-005-1 R1 (RFC2011001149, RFC2011001158 and RFC2011001166)

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."

CIP-005-1 R1 provides:

> R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> > R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
> >
> > R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
> >
> > R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
> >
> > R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.
> >
> > R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

> R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

CIP-005-1 R1 has a "Medium" VRF[7] and a "Severe" VSL.

During the Compliance Audit, Reliability*First* and MRO discovered that the UREs failed to identify and document the Electronic Security Perimeter (ESP). The switches in the UREs' telecommunications and server rooms had many network connections that were enabled but that the UREs were unable to identify. Specifically, at the first control center, the ESP switch should have only had a certain number of active connections enabled but had more active connections hard-wired connections enabled. At the second control center, the ESP switch should have only had a certain number of active connections enabled but had more active connections hard-wired connections enabled. The UREs were unaware of these additional connections that were actively transmitting information and which should have been included within the ESP and documented as such. As a result, the UREs failed to identify and document its ESP, as required by CIP-005-1 R1.

Additionally, the UREs had dual network printers at both its control centers that constitute access points to the ESPs. However, the UREs failed to identify and document these access points to the ESPs, as required by CIP-005-1 R1.

The UREs also failed to maintain documentation of certain non-critical Cyber Assets within the ESPs, as required by CIP-005-1 R1.4. Specifically, the UREs failed to document several printers at the affected control centers.

Lastly, the UREs failed to maintain documentation of all Cyber Assets within the ESP, as required by CIP-005-1 R1.6.

Reliability*First* determined that the UREs had violations of CIP-005-1 R1 because they failed to: (a) identify and document the ESP; (b) identify and document certain access points to the ESP; and (c) maintain documentation of certain Cyber Assets within the ESP.

[7] CIP-005-1 R1 has a "Medium" VRF, as do subrequirements R1.1 through R1.5. R1.6 has a "Lower" VRF.

ReliabilityFirst determined the duration of the violations to be the date the Standard became mandatory and enforceable for the UREs through when the UREs completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The violations posed a moderate risk because they provide the opportunity for cyber intrusions to occur on CCAs located outside an established ESP. However, the risk was mitigated by the fact that the UREs had multiple layers of protection in place for their ESPs. For example, each substation has an identifiable router that uses virtual local area network connections to segregate the CCAs from the non-critical items to which maintenance workers require access. In addition, each device is located at the substation behind a fence and in a locked building with key-card access. Each device is located within a separate locked cabinet that provided an alarm to the monitoring group upon opening. Further, the printers in the control centers are protected by firewall security, isolation by virtual network configuration, and restricted physical access to the Physical Security Perimeter (PSP).

CIP-005-1 R2 (RFC2011001150, RFC2011001159 and RFC2011001167)
CIP-005-1 R2 provides:

> 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).
>
> R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
>
> 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.
>
> R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
>
> R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or

technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

CIP-005-1 R2 has a "Medium" VRF[8] and a "Severe" VSL.

During the Compliance Audit, Reliability*First* and MRO discovered that the procedures the UREs had in place did not include the detail required to constitute organizational processes and technical and procedural mechanisms for control of electronic access at all access points to the ESP. The procedures involved a high-level description of the organizational processes and technical and procedural mechanisms for control of electronic access at all access points to the ESP, but did not state how the UREs would implement these mechanisms in detail. As a result, the UREs failed to document and implement the processes and mechanisms required by CIP-005-1 R2.

In addition, the UREs have in place a server that centralizes the access control mechanisms for the UREs' system, which allows authentication of users attempting to access deployed network hardware or distributed resources. For this server, which enables external interactive access into the ESP, it was not technically feasible for the UREs to implement strong procedural or technical controls at the access

[8] CIP-005-1 R2 has a "Medium" VRF, as do subrequirements R2.1 through R2.4. R2.5 and all of its subrequirements, as well as R2.6, have a "Lower" VRF.

points to ensure authenticity of the accessing party, as required by CIP-005-1 R2.4. The UREs failed to submit a Technical Feasibility Exception (TFE) to Reliability*First*.

Reliability*First* determined that the UREs had violations of CIP-005-1 R2 because they failed to: (a) implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESP and (b) implement strong procedural or technical controls at the access points where external interactive access into the ESP has been enabled to ensure authenticity of the accessing party.

Reliability*First* determined the duration of the CIP-005-1 R2.4 violations to be from the date the Standard became mandatory and enforceable for the UREs through when Reliability*First* and MRO approved the UREs' TFE request.

Reliability*First* determined the duration of the remaining CIP-005-1 R2 violations to be from the date the Standard became mandatory and enforceable through the date the UREs revised the documentation.

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. The violations posed a moderate risk because they provided the opportunity for inconsistent application of organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESP. Such inconsistent application can leave access points, and therefore the ESP, exposed to unauthorized access and vulnerable to cyber intrusion. However, the risk was mitigated by the fact that although the UREs failed to document the technical and procedural controls, the UREs were performing the required controls. Additionally, for the transmission management system ESPs, the firewalls limit interactive access to only restricted virtual consoles and authentication by the transmission management system applications and systems within the ESP. For the substation ESPs, there are access control rules that filter the network traffic through the firewall and that only allow appropriate traffic through the firewall.

<u>CIP-005-1 R4 (RFC2011001160)</u>
CIP-005-1 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; and,

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-005-1 R4 has a "Medium" VRF[9] and a "Severe" VSL.

During the Compliance Audit, Reliability*First* discovered that URE2 failed to include the access points to some of its substations' ESPs in its cyber vulnerability assessment (CVA) for one year.

Reliability*First* determined that URE2 had a violation of CIP-005-1 R4.3 because URE2 failed to include the discovery of all access points to the ESP in its CVA.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE2 through when URE2 completed its Mitigation Plan.

Reliability*First* determined that the violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The violation posed a moderate risk because it provides the opportunity for individuals to exploit vulnerabilities of ESP access points of which URE2 may be unaware. By exploiting vulnerabilities which would have been discoverable and preventable through the application of an annual CVA, an individual could gain unauthorized access to CCAs within the ESP and cause harm to the integrity of the CCAs. However, the risk was mitigated by the fact that the substations at issue had the same access control requirements as all other sites scanned during the CVA, including firewalls and isolation by virtual network configuration. As a result, the CVA considered the same devices as those present at the affected substations, and Reliability*First* discovered no additional issues with URE2's CVAs. In addition, remote access to the substations is limited to a small

[9] CIP-005-1 R4 has a "Medium" VRF, as do subrequirements R4.2 through R4.5. R4.1 has a "Lower" VRF.

subset of users with appropriate credentials, reducing the likelihood that an unauthorized user would access the substation unnoticed.

CIP-005-1 R5 (RFC2011001152, RFC2011001161 and RFC2011001169)

CIP-005-1 R5 provides:

> R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.
>
> R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
> R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
>
> R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

CIP-005-1 R5 has a "Lower" VRF and a "Severe" VSL.

During the Compliance Audit, Reliability*First* and MRO discovered that the UREs failed to ensure that certain documentation required by the Standard reflected current configurations. The UREs' procedure describes the integrated security solution implemented by the UREs for controlling, monitoring, and logging electronic access at all ESP access points 24 hours a day. The UREs failed to ensure that the procedure contained figures reflective of the UREs' current configuration.

Reliability*First* determined that the UREs had violations of CIP-005-1 R5 because they failed to ensure that certain documentation required by the Standard reflected current configurations.

Reliability*First* determined the duration of the CIP-005-1 R5 violations to be from the date the Standard became mandatory and enforceable for the UREs through when the UREs completed their Mitigation Plans.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS because the figures are high-level representations UREs' integrated security solution and not detailed descriptions of access points to the ESPs. The UREs use other detailed diagrams to depict actual access points to the control center and substation ESPs. In addition, the remainder of the procedure reflected current configurations and processes.

CIP-006-1 R1 (RFC2011001153, RFC2011001162 and RFC2011001170)

The purpose statement of Reliability Standard CIP-006-1 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."

CIP-006-1 R1 provides:

> 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.
> >
> > R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.
> >
> > R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).
> >
> > R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
> >
> > R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

CIP-006-1 R1 has a "Medium" VRF[10] and a "Severe" VSL.

During the Compliance Audit, Reliability*First* and MRO discovered several instances of non-compliance with CIP-006-1 R1. First, at a control center, the UREs failed to establish a six-wall border between the maintenance hall and an adjacent conference room. The wall above the drop-ceiling did not fully extend to the concrete ceiling above, creating a gap. In addition, at a UREs' control center, there was a gap located under one wall of the PSP. As a result, the UREs failed to ensure that these Cyber Assets within the ESP reside within an identified PSP, as required by CIP-006-1 R1.1.

Second, the UREs failed to deploy and document alternative measures to control physical access to Cyber Assets where a completely enclosed border could not be established. At the UREs' control center, one cable connects a computer lab and the server room, which are all located within one ESP. The UREs failed to locate this cable, which is a Cyber Asset within the ESP, within a defined PSP, as required by CIP-006-1 R1.1. In addition, the same configuration exists at the UREs' other control center. Furthermore, the other control center and the server room at the other control center are connected by a cable between the first control center and a telecommunications room. However, the

[10] CIP-006-1 R1 has a "Medium" VRF, as do subrequirements R1.1 through R1.6. CIP-006-1 R1.7 through R1.9 have a "Lower" VRF.

telecommunications room was not a defined PSP, and as a result, the cable, which is a Cyber Asset within an ESP, was not located within a defined PSP, as required by CIP-006-1 R1.1.

Third, at URE2's substation, where a completely enclosed (six-wall) border cannot be established, URE2 utilizes wireless radio signals to communicate between the CCAs and the control house at the substation. However, these radio signals extend beyond a PSP. URE2 failed to deploy and document alternative measures to control physical access to these radio signals, as required by CIP-006-1 R1.1.

Fourth, the UREs' physical security plan does not identify physical access points through each PSP and measures to control entry at those access points. The UREs maintained a document containing identification of all physical access points through each PSP. However, that document had the following deficiencies: (a) the physical security plan does not reference it; (b) the UREs do not annually review it; (c) it is not specific enough to determine the actual boundary of the PSP for the control centers, server rooms, or labs; and (d) it fails to identify two of the four doors to the control center as access points (the UREs identified these doors as "exit only" doors rather than access points). Therefore, the UREs failed to include in their physical security plan the identification of all physical access points through each PSP and measures to control entry at those access points, as required by CIP-006-1 R1.2.

Reliability*First* determined that the UREs had violations of CIP-006-1 R1 because they failed to: (a) ensure all Cyber Assets within the ESP reside within an identified PSP and (b) deploy and document alternative measures to control physical access to Cyber Assets within the ESP where they could not establish a completely enclosed (six-wall) border.

With respect to the gaps in the six-wall border, Reliability*First* determined the duration of the CIP-006-1 R1 violations to be from the date the Standard became mandatory and enforceable for the UREs through when the UREs closed the gaps. Reliability*First* determined the duration of the remainder of the CIP-006-1 R1 violations to be from the date the Standard became mandatory and enforceable for the UREs 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. The violations posed a moderate risk because they provide the opportunity to physically access Cyber Assets that are not protected by the implementation of a physical security plan. However, the risk was mitigated by the fact that all of the access points to the PSPs at the control centers were properly secured with access control and monitoring. Specifically, the UREs protect access to the control center through an access control system at the main entrance onto the site, into the headquarters building, and onto the specific floors. In addition, there are video

cameras situated on the exterior of the building that view important access points into and within the building. The access control system and video camera system are fully integrated into the UREs' security system, and trained security professionals monitor them 24 hours a day. Furthermore, there are a variety of natural and artificial barriers surrounding the perimeter of the control center campus. The other control center has similar protections in place, including interior and exterior video cameras, perimeter fencing, and an access control system at the main entrance onto the site and into the main structure. All of the other control center's physical security systems are integrated into the UREs' security system, and trained professionals monitor them 24 hours a day.

The UREs had multiple layers of protection in place for their ESPs, which also mitigated the risk caused by the violations. For example, each substation has an identifiable router that used virtual local area network connections to segregate the CCAs from the non-critical items to which maintenance workers required access. In addition, each device is located at the substation behind a fence and in a locked building requiring key-card access. Each device was located within a separate locked cabinet that provided an alarm to the monitoring group upon opening.

Regarding the violation of CIP-006-1 R1.2, the risk was mitigated by the fact that the UREs had documented the access points to the PSPs (which includes the inadequate identification of the two doors as "exit only"). The UREs were monitoring and updating changes despite failing to include or reference this in the physical security plan.

CIP-007-1 R3 (RFC2011001154, RFC2011001163 and RFC2011001171)

The purpose statement of Reliability Standard CIP-007-1 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 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.

During the Compliance Audit, Reliability*First* and MRO discovered that the UREs established, documented and implemented a security patch management program. However, the UREs failed to include the tracking of applicable cybersecurity software patches for all Cyber Assets within the ESP in its program.

Reliability*First* determined that the UREs had violations of CIP-007-1 R3 because they failed to establish, document, and implement a security patch management program for tracking applicable cybersecurity software patches for all Cyber Assets within the ESP.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the UREs through when the UREs completed their 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. The violations posed a moderate risk because they provide the opportunity for infiltration of unauthorized network traffic into the ESP when security patches and upgrades are not installed on Cyber Assets within the ESP. However, the risk was mitigated by the fact that the UREs have TFEs for the majority of their CCAs regarding security patching. The UREs also have a defense-in-depth strategy where they protect access to CCAs with firewalls, isolation by virtual network configuration, a required corporate user identification and password, and physical security controls. For those CCAs that do not have TFEs, the UREs evaluate all patches within 30 calendar days of applicability, as required by CIP-007-1 R3.

CIP-007-1 R5 (RFC2011001155, RFC2011001164 and RFC2011001172)

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).
>
> R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:
>
> > R5.3.1. Each password shall be a minimum of six characters.
> >
> > R5.3.2. Each password shall consist of a combination of alpha, numeric, and “special” characters.
> >
> > R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

CIP-007-1 R5 has a "Medium" VRF[11] and a "Severe" VSL.

During the Compliance Audit, Reliability*First* and MRO discovered several deficiencies with the UREs' account and password management policies. The UREs implemented a policy that recommended, but did not require, steps to minimize and manage the scope and acceptable use of generic and administrator accounts. Specifically, the UREs' policy recommended, but did not require: (a) the removal, disabling or renaming of generic and administrator accounts and (b) the changing of passwords for such accounts that must remain enabled prior to putting any system into service, as required by CIP-007-1 R5.2.1.

Second, the UREs' policy to minimize and manage the scope and acceptable use of shared accounts did not include steps for securing shared accounts in the event of personnel changes for its integrated security solution, substations or physical security system, as required by CIP-007-1 R5.2.3. Specifically, the UREs' policy did not require passwords to be changed in the event of personnel changes for its integrated security solution, substations or physical security system.

Third, for its substations, the UREs' password management policy defines "strong" passwords as those that contain at least eight characters and are comprised of alphabetic, numeric and special characters. However, the UREs' policy allows certain types of passwords for read-only access, but these passwords only required four characters. As a result, the UREs failed to require and use passwords compliant with CIP-007-1 R5.3.1, R5.3.2, and R5.3.3.

Fourth, the UREs' corporate password management policy requires passwords to contain at least three of the following four character groups: upper-case alphabetic letters, lower-case alphabetic letters, special characters, and numeric characters. As a result, the UREs do not require passwords to consist of a combination of alpha, numeric and special characters, as required by CIP-007-1 R5.3.2.

Reliability*First* determined that the UREs had violations of CIP-007-1 R5 because they failed to: (a) implement a policy that includes the removal, disabling or renaming of generic and administrator accounts; (b) implement a policy that requires passwords to be changed for generic or administrator accounts where those accounts must remain enabled; (c) include steps for securing shared accounts in the event of personnel changes; and (d) require and use passwords which were compliant with CIP-007-1 R5.

[11] CIP-007-1 R5 has a "Lower" VRF, as do R5.2, R5.2.2, R5.3, R5.3.1, and R5.3.2. CIP-007-1 R5.2.1, R5.2.3, and R5.3.3 have a "Medium" VRF. CIP-007-1 R5.1 is not at issue here.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the UREs through the present.

ReliabilityFirst determined that the violations of CIP-007-1 R5.2.1, R5.2.3 and R5.3 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The violations posed a moderate risk because they provide the opportunity for unauthorized system access. However, the risk was mitigated by the fact that although the UREs failed to document effectively the shared account password changes, they were changing the passwords when personnel changes occurred.

ReliabilityFirst determined that the CIP-007-1 R5.3.2 violations posed a minimal risk and not serious or substantial risk to the reliability of the BPS. The UREs' corporate password management policy requires passwords to contain a combination of upper-case alphabetic letters, lower-case alphabetic letters, special characters, and numeric characters. Although the specific policy does not meet the requirements of CIP-007-1 R5.3.2, the passwords created using the UREs' policy were strong. The UREs protect the devices for which it is technically infeasible to enforce password requirements through other means, such as the security command center, which sends an alarm and terminates communication if there is any attempt to alter a device. Where it was technically infeasible, the UREs submitted TFEs.

CIP-007-1 R9 (RFC2011001156, RFC2011001165 and RFC2011001173)

CIP-007-1 R9 provides: "Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change."

CIP-007-1 R9 has a "Lower" VRF and a "High" VSL.

During the Compliance Audit, ReliabilityFirst and MRO discovered that the UREs failed to document changes resulting from certain modifications to its systems or controls within 30 calendar days of such changes. The UREs failed to: (a) revise its integrated security solution policy to reflect the decommissioning of a certain device; (b) create a list of non-critical Cyber Assets; and (c) update test plans in the change management test track process related to Cyber Assets.

ReliabilityFirst determined that the UREs had violations of CIP-007-1 R9 because they failed to document changes resulting from modifications to the systems or controls within 30 calendar days of the change being completed.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the UREs through when the UREs' Mitigation Plans were completed.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The violations posed a moderate risk because the UREs utilized cybersecurity documentation that was not up-to-date. However, the risk was mitigated by the fact that the UREs made modifications to their system as they deemed necessary, and the violation resulted from a failure to document those changes. Additionally, no cybersecurity incidents occurred on the UREs' system during the time of the violations.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of one hundred twenty thousand dollars ($120,000) for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors:

1. ReliabilityFirst considered the UREs' violation history as an aggravating factor in the penalty determination;
2. The UREs had an internal compliance program (ICP) at the time of the violations which ReliabilityFirst considered a mitigating factor;
3. The UREs are undertaking efforts to improve their CIP ICP, which demonstrates a commendable commitment to sustainable compliance, and for which ReliabilityFirst applied significant mitigating credit;
4. ReliabilityFirst determined that the violations of CIP-005-1 R5 and CIP-007-1 R5 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS, and that the violations of CIP-004-1 R2; CIP-005-1 R1, R2, and R4; CIP-006-1 R1; and CIP-007-1 R3 and R9 posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
5. ReliabilityFirst reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of one hundred twenty thousand dollars ($120,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[12]

RFCMIT007490 (RFC2011001148), RFCMIT007489 (RFC2011001157)
URE1 and URE2's Mitigation Plans to address their violations of CIP-004-1 R2 were submitted to Reliability*First*. The Mitigation Plans were accepted by Reliability*First* and approved by NERC. The Mitigation Plans for these violations are designated as RFCMIT007490 and RFCMIT007489 and were submitted as non-public information to FERC in accordance with FERC orders.

URE1 and URE2's Mitigation Plans required URE1 and URE2 to require third-party entities to complete the cybersecurity awareness training.

URE1 and URE2 certified that the above Mitigation Plan requirement was completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of URE1 and URE2's submitted evidence, Reliability*First* verified that the URE1 and URE2's Mitigation Plan was completed.

RFCMIT007409 (RFC2011001149), RFCMIT007408 (RFC2011001158), RFCMIT007410 (RFC2011001166)
The UREs' Mitigation Plans[13] to address their violations of CIP-005-1 R1 were submitted to Reliability*First*. The Mitigation Plans were accepted by Reliability*First* and approved by NERC. The Mitigation Plans for these violations are designated as RFCMIT007409, RFCMIT007408 and RFCMIT007410, respectively, and were submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plans required the UREs to:

1. Correct the diagrams and re-publish the documents;
2. Reorganize all connections and ports to the ESP switches in the operations centers to accurately reflect the documented configurations and remove undocumented connections to control center switches;
3. Implement and document controls whereby they will disable an unused switch port by default and require a request before any new ports may be enabled and used;
4. Review evidence and take corrective actions as needed after comparing active ports to required ports to remediate differences; and

[12] *See* 18 C.F.R § 39.7(d)(7).
[13] Mitigation Plans RFCMIT007409, RFCMIT007408, and RFCMIT007410 are identical.

5. Conduct a lessons learned meeting to discuss and review the implementation of corrective actions as they apply to disabling switch ports.

The UREs certified that the above Mitigation Plan requirements were completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that the UREs' Mitigation Plan was completed.

RFCMIT007493 (RFC2011001150), RFCMIT007491 (RFC2011001159), RFCMIT007494 (RFC2011001167)
The UREs' Mitigation Plans[14] to address their violations of CIP-005-1 R2 were submitted to Reliability*First*. The Mitigation Plans were accepted by Reliability*First* and approved by NERC. The Mitigation Plans for these violations are designated as RFCMIT007493, RFCMIT007491 and RFCMIT007494, respectively, and were submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plans required the UREs to:

1. Enhance procedures to clearly describe the technical and procedural mechanisms used for control of electronic access at all electronic access points to the ESP; and
2. File TFEs, as necessary.

The UREs certified that the above Mitigation Plan requirements were completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that the UREs' Mitigation Plan was completed.

RFCMIT007492 (RFC2011001160)
URE2's Mitigation Plan to address its violation of CIP-005-1 R4 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 RFCMIT007492 and was submitted as non-public information to FERC in accordance with FERC orders.

[14] Mitigation Plans RFCMIT007493, RFCMIT007491 and RFCMIT007494 are identical.

URE2's Mitigation Plan required URE2 to:

1. Revise its CVA process to ensure that it includes all predetermined access points to the ESP;
2. Develop a checklist method to accompany the revised process; and
3. Provide training on the revisions to the process.

URE2 certified that the above Mitigation Plan requirements were completed. URE2 submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of URE2's submitted evidence, Reliability*First* verified that URE2's Mitigation Plan was completed.

RFCMIT007478-1 (RFC2011001152), RFCMIT007487 (RFC2011001161), RFCMIT007488 (RFC2011001169)

URE2 and URE3's Mitigation Plans to address their violations of CIP-005-1 R5 were submitted to Reliability*First*. The Mitigation Plans were accepted by Reliability*First* and approved by NERC. The Mitigation Plans for these violations are designated as RFCMIT007487 and RFCMIT007488, respectively, and were submitted as non-public information to FERC in accordance with FERC orders.

URE1's Mitigation Plan to address its violation of CIP-005-1 R5 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 RFCMIT007478-1 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plans[15] required the UREs to:

1. Correct the CIP-077 integrated security solution diagrams;
2. Republish the diagrams; and
3. Conduct a quarterly review of the policies schedule.

The UREs certified that the above Mitigation Plan requirements were completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that the UREs' Mitigation Plan was completed.

[15] Mitigation Plans RFCMIT007492, RFCMIT007478-1, and RFCMIT007488 are identical.

RFCMIT007630 (RFC2011001153), RFCMIT007629 (RFC2011001162), RFCMIT007631 (RFC2011001170)
The UREs' Mitigation Plans to address their violations of CIP-006-1 R1 were submitted to Reliability*First*. The Mitigation Plans were accepted by Reliability*First* and approved by NERC. The Mitigation Plans for these violations are designated as RFCMIT007630, RFCMIT007629, and RFCMIT007631, and were submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plans required the UREs to:

1. Revise their physical security plan and testing and maintenance procedure for physical security mechanisms to stipulate that CCAs within an ESP must reside within a single ESP or have appropriate protection when an ESP spans multiple PSPs;
2. Define a new annual physical inspection process including:
    a. An annual tabletop review;
    b. A physical inspection of all ESPs to ensure they reside in a PSP;
    c. Development of a corrective action plan to mitigate findings from the annual physical inspection; and
    d. Completion of all corrective actions discovered from the inspection; and
3. Create a new document that clearly identifies all physical access points for all PSPs.

In addition to the actions outlined in the Mitigation Plans, the UREs remediated certain aspects of the violations during the Compliance Audit. Specifically, the UREs:

1. Closed the gap in the ceiling of the PSP at the Control Center; and
2. Closed the gap between the wall and the floor of the PSP at the Control Center.

URE2 also submitted a TFE for the wireless radio signals to communicate between the CCAs and the control house at the affected substation. Reliability*First* accepted and approved the TFE.

RFCMIT007666 (RFC2011001154), RFCMIT007663 (RFC2011001163), RFCMIT007668 (RFC2011001171)
The UREs' Mitigation Plans[16] to address their violations of CIP-007-1 R3 were submitted to Reliability*First*. The Mitigation Plans were accepted by Reliability*First* and approved by NERC. The Mitigation Plans for these violations are designated as RFCMIT007666, RFCMIT007663 and

[16] Mitigation Plans RFCMIT007666, RFCMIT007663 and RFCMIT007668 are identical.

RFCMIT007668, respectively, and were submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plans required the UREs to:

1. Submit TFEs for those CCAs that require them;
2. Revise their security patch tracking procedure to include patch tracking; and
3. Implement a patch notification and analysis tracking process for their Transmission Management System, integrated security solution, physical security system, and engineering department.

The UREs certified that the above Mitigation Plan requirements were completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that UREs' Mitigation Plan was completed.

RFCMIT007729 (RC2011001155), RFCMIT007728 (RFC2011001164), RFCMIT007730 (RFC2011001172)
The UREs' Mitigation Plans[17] to address their violations of CIP-007-1 R5 were submitted to Reliability*First*. The Mitigation Plans were accepted by Reliability*First* and approved by NERC. The Mitigation Plans for these violations are designated as RFCMIT007729, RFCMIT007728 and RFCMIT007730, respectively, and were submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to:

1. Revise their password standards document to require:
    a. The removal, disabling, or renaming of generic or administrator accounts where technically feasible,
    b. That individuals change all passwords prior to placing any system into service for accounts that must remain enabled, and
    c. That all password changes for generic or administrator accounts be recorded in the change management tool,

[17] Mitigation Plans RFCMIT007729, RFCMIT007728 and RFCMIT007730 are identical.

2. Revise their account management and logging policy to require the changing of all shared accounts' passwords in the event of personnel changes for all areas including the integrated security solution, substations, physical security system, and Transmission Management System;
3. Create a process describing how they will document and implement password changes for shared accounts;
4. Redesign the password generator to comply with the password requirements;
5. Review the current methods employed and industry guidelines to develop a solution with the vendor, which entails:
    a. Creating a common strong unique password for relevant assets,
    b. Utilizing the new password,
    c. Allowing for all relevant assets' passwords to be managed or reset on a substation-by-substation basis to allow for a second quarter annual reset, and
    d. Filing TFEs for those assets not capable of creating compliant passwords; and
6. Filing all necessary TFEs.

RFCMIT007665 (RFC2011001156), RFCMIT007664 (RFC2011001165), RFCMIT007667 (RFC2011001173)
The UREs' Mitigation Plans[18] to address their violations of CIP-007-1 R9 were submitted to Reliability*First*. The Mitigation Plans were accepted by Reliability*First* and approved by NERC. The Mitigation Plans for these violations are designated as RFCMIT007665, RFCMIT007664 and RFCMIT007667, respectively, and were submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plans required the UREs to:

1. Update the integrated security solution to remove the quality assurance system from all diagrams and update the Cyber Assets used for access control or monitoring of ESP or PSP;
2. Enhance test plans for each business area to incorporate the change management process such that it captures test results as part of the audit trail; and
3. Revise their documentation review process so that the workload is distributed throughout the year rather than during the third quarter so that the personnel can better ensure they maintain the necessary updates.

[18] Mitigation Plans RFCMIT007665, RFCMIT007664 and RFCMIT007667 are identical.

The UREs certified that the above Mitigation Plan requirements were completed. The UREs submitted evidence of completion of their Mitigation Plan.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that UREs' Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[19]

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,[20] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on March 12, 2013. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of a one hundred twenty thousand dollar ($120,000) financial penalty against the UREs 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. The violations constituted repeat violations of some of the subject NERC Reliability Standards by the UREs and Reliability*First* considered the UREs' violation history as an aggravating factor in the penalty determination;
2. The UREs had a compliance program at the time of the violation which Reliability*First* considered a mitigating factor, as discussed above;
3. The UREs are undertaking efforts to improve their CIP ICP, which demonstrates a commendable commitment to sustainable compliance, and for which Reliability*First* applied significant mitigating credit;

[19] *See* 18 C.F.R. § 39.7(d)(4).
[20] *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. Reliability*First* determined that the violations of CIP-005-1 R5 and CIP-007-1 R5 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS, and that the violations of CIP-004-1 R2; CIP-005-1 R1, R2, and R4; CIP-006-1 R1; and CIP-007-1 R3 and R9 posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
5. 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 one hundred twenty thousand dollars ($120,000) 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 the UREs executed August 22, 2012, included as Attachment a;

b) Record documents for the violations of CIP-004-1 R2 (RFC2011001148 and RFC2011001157), included as Attachment b:

   1. URE1's Mitigation Plan designated as RFCMIT007490;
   2. URE2's Mitigation Plan designated as RFCMIT007489;
   3. URE1's Certification of Mitigation Plan Completion;
   4. URE2's Certification of Mitigation Plan Completion;
   5. Reliability*First*'s Verification of Mitigation Plan Completion;

c) Record documents for the violations of CIP-005-1 R1 (RFC2011001149, RFC2011001158, and RFC2011001166), included as Attachment c:

   1. URE1's Mitigation Plan designated as RFCMIT007409;
   2. URE2's Mitigation Plan designated as RFCMIT007408;
   3. URE3's Mitigation Plan designated as RFCMIT007410;
   4. URE1's Certification of Mitigation Plan Completion;
   5. URE2's Certification of Mitigation Plan Completion;
   6. URE3's Certification of Mitigation Plan Completion;
   7. Reliability*First*'s Verification of Mitigation Plan Completion;

d) Record documents for the violations of CIP-005-1 R2 (RFC2011001150, RFC2011001159, and RFC2011001167), included as Attachment d:

   1. URE1's Mitigation Plan designated as RFCMIT007493;
   2. URE2's Mitigation Plan designated as RFCMIT007491;
   3. URE3's Mitigation Plan designated as RFCMIT007494;
   4. URE1's Certification of Mitigation Plan Completion;
   5. URE2's Certification of Mitigation Plan Completion;

6. URE3's Certification of Mitigation Plan Completion;
7. Reliability*First*'s Verification of Mitigation Plan Completion;

e) Record documents for the violation of CIP-005-1 R4 (RFC2011001160), included as Attachment e:

1. URE2's Mitigation Plan designated as RFCMIT007492;
2. URE2's Certification of Mitigation Plan Completion;
3. Reliability*First*'s Verification of Mitigation Plan Completion;

f) Record documents for the violations of CIP-005-1 R5 (RFC2011001152, RFC2011001161, and RFC2011001169), included as Attachment f:

1. URE1's Mitigation Plan designated as RFCMIT007478-1;
2. URE2's Mitigation Plan designated as RFCMIT007487;
3. URE3's Mitigation Plan designated as RFCMIT007488;
4. URE1's Certification of Mitigation Plan Completion;
5. URE2's Certification of Mitigation Plan Completion;
6. URE3's Certification of Mitigation Plan Completion;
7. Reliability*First*'s Verification of Mitigation Plan Completion;

g) Record documents for the violations of CIP-006-1 R1 (RFC2011001153, RFC2011001162, RFC2011001170), included as Attachment g:

1. URE1's Mitigation Plan designated as RFCMIT007630;
2. URE2's Mitigation Plan designated as RFCMIT007629;
3. URE3's Mitigation Plan designated as RFCMIT007631;

h) Record documents for the violations of CIP-007-1 R3 (RFC2011001154, RFC2011001163, and RFC2011001171), included as Attachment h:

1. URE1's Mitigation Plan designated as RFCMIT007666;
2. URE2's Mitigation Plan designated as RFCMIT007663;
3. URE3's Mitigation Plan designated as RFCMIT007668;
4. URE1's Certification of Mitigation Plan Completion;
5. URE2's Certification of Mitigation Plan Completion;

6. URE3's Certification of Mitigation Plan Completion;
7. Reliability*First*'s Verification of Mitigation Plan Completion;

i) Record documents for the violation of CIP-007-1 R5 (RFC2011001155, RFC2011001164, and RFC2011001172), included as Attachment i:

1. URE1's Mitigation Plan designated as RFCMIT007729;
2. URE2's Mitigation Plan designated as RFCMIT007728;
3. URE3's Mitigation Plan designated as RFCMIT007730;

j) Record documents for the violation of CIP-007-1 R9 (RFC2011001156, RFC2011001165, and RFC2011001173), included as Attachment j:

1. URE1's Mitigation Plan designated as RFCMIT007665;
2. URE2's Mitigation Plan designated as RFCMIT007664;
3. URE3's Mitigation Plan designated as RFCMIT007667;
4. URE1's Certification of Mitigation Plan Completion;
5. URE2's Certification of Mitigation Plan Completion;
6. URE3's Certification of Mitigation Plan Completion; and
7. Reliability*First*'s Verification of Mitigation Plan Completion.

A Form of Notice Suitable for Publication[21]

A copy of a notice suitable for publication is included in Attachment k.

[21] *See* 18 C.F.R § 39.7(d)(6).

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 (330) 456-2488 bob.wargo@rfirst.org L. Jason Blake* General Counsel Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 jason.blake@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* Senior Counsel and Associate 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 edwin.kichline@nerc.net Megan E. Gambrel* Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 megan.gambrel@rfirst.org

	Michael D. Austin* Managing Enforcement Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 mike.austin@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 C. 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
charlie.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
Senior Counsel and Associate 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
edwin.kichline@nerc.net

cc: Unidentified Registered Entities
ReliabilityFirst Corporation

Attachments