PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

October 31, 2012

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), , Unidentified Registered Entity 2 (URE2), and Unidentified Registered Entity 3 (URE3), (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]

As subsidiaries of the same corporation and subject to many of the same processes and procedures implemented by their parent company, many of the facts and circumstances of the instant violations[3] apply to all three registered entities. This similarity of violations occurs most frequently for the violations with respect to URE2 and URE3, due to their use of the same programs and procedures relating to the Critical Infrastructure Protection (CIP) Reliability Standards. Additionally, this similarity of violations occurs frequently between URE1, URE2 and URE3, which again utilize the same programs and procedures related to the CIP Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (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.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

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 that the following standards have been violated: CIP-002-1 Requirements (R)1, R2, R3, and R4;[4] CIP-003-1 R1, R5, and R6; CIP-004-1 R1, R3, and R4; CIP-004-2 R2; CIP-005-1 R1, R2, R3, R4, and R5; CIP-006-1 R1; CIP-007-1 R1, R2, R3, R4, R5, R6, and R8; CIP-008-1; R1; and CIP-009-1 R1, R2, R3, R4, and R5. According to the Settlement Agreement, the UREs neither admit nor deny the violations, but have agreed to the assessed penalty of seven hundred twenty-five thousand dollars ($725,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers RFC201000540, RFC201000561, RFC201000582, RFC201100957, RFC201100958, RFC201100959, RFC201100960, RFC201100961, RFC201100962, RFC201100963, RFC201100964, RFC201100965, RFC201100966, RFC201100967, RFC201100968, RFC201100969, RFC201100970, RFC201100971, RFC201100972, RFC201100973, RFC201100974, RFC201100975, RFC201100976, RFC201100977, RFC201100978, RFC201100979, RFC201100981, RFC201100982, RFC201100983, RFC201100984, RFC201100985, RFC201100986, RFC201100987, RFC2011001178, RFC2011001179, RFC2011001180, RFC2011001181, RFC2011001182, RFC2011001183, RFC2011001184, RFC2011001185, RFC2011001186, RFC2011001187, RFC2011001274, RFC2011001275, RFC2011001276, RFC2011001277, RFC2011001278, RFC2011001279, RFC2011001280, RFC2011001281, RFC2011001282, RFC2011001283, RFC2011001284, RFC2011001285, RFC2011001286, RFC2011001287, RFC2011001288, RFC2011001289, RFC2011001290, RFC2011001291, RFC2011001292, RFC2011001293, RFC2011001294, RFC2011001295, RFC2011001296, RFC2011001299, RFC2011001300, RFC2012009913, RFC2012009914, RFC2012009915, RFC2012010075, and RFC2012010076 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

In the aggregate, the UREs' failure to document the full range of protections afforded in CIP-002-1 through CIP-009-1 and to implement the processes and procedures through which these protections are maintained presented the potential for substantial risk to the reliability of the bulk power system (BPS) through compromised integrity of their Critical Cyber Assets (CCAs). As a result, Reliability*First* did not offer, and the UREs did not request, classification of the violations in a Find, Fix, Track, and Report filing. However, the aggregate risk posed by the UREs' violations is not ongoing, due to the

[4] CIP Version 1 became effective on July 1, 2008 and remained enforceable through March 31, 2010. CIP Version 2 was approved by the Commission and became enforceable on April 1, 2010 and was enforceable through September 30, 2010. CIP Version 3 was approved by the Commission and became enforceable on October 1, 2010 and remained enforceable through the end duration date of the CIP violations included in this filing. For consistency in this document, the violations reference the earliest version of the CIP Standard for each violation. Except as noted, the fact that more than one version of the CIP Standards was effective had no bearing on the violations addressed herein.

UREs' implementation of Mitigation Plans, as described below, and implementation of a compliance initiative, which revised their CIP compliance program. All of these risk factors have been taken into consideration in conjunction with the Settlement Agreement.

Due to the aggregate risk posed by these violations, Reliability*First* and the UREs collaborated to immediately assess and address the violations. For example, Reliability*First* executives engaged executives of the UREs to ensure the UREs' organizational commitment to address the violations. The UREs participated in numerous meetings and conferences with Reliability*First* personnel to discuss the UREs' progress in mitigating the violations.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement by and between Reliability*First* and the UREs, which is included as Attachment a. The details of the findings and the 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 (2012), 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.	VRF	Total Penalty
Reliability*First* Corporation	URE1	1448	RFC201100957	CIP-002-1	R1	Medium[5]	$725,000
Reliability*First* Corporation	URE1	1448	RFC201100958	CIP-002-1	R2	High[6]	

[5] When NERC filed Violation Risk Factors (VRFs) it originally assigned CIP-002-1 R1 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-002-1 R1 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

[6] When NERC filed VRFs it originally assigned CIP-002-1 R2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on January 27, 2009, the Commission approved the modified High VRF. Therefore, the Lower VRF for CIP-002-1 R2 was in effect from June 18, 2007 until January 27, 2009 when the High VRF became effective.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req.	VRF	Total Penalty
Reliability*First* Corporation	URE1	1448	RFC201100959	CIP-002-1	R3	High[7]	
Reliability*First* Corporation	URE1	1448	RFC201100960	CIP-002-1	R4	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100961	CIP-003-1	R1	Medium[8]	
Reliability*First* Corporation	URE1	1448	RFC201100962	CIP-003-1	R5	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100963	CIP-003-1	R6	Lower	
Reliability*First* Corporation	URE2	1448	RFC2011001274	CIP-003-1	R6	Lower	
Reliability*First* Corporation	URE3	1448	RFC2011001275	CIP-003-1	R6	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100964	CIP-004-1	R1	Lower	
Reliability*First* Corporation	URE2	1448	RFC2011001276	CIP-004-1	R1	Lower	
Reliability*First* Corporation	URE3	1448	RFC2011001277	CIP-004-1	R1	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100965	CIP-004-2	R2	Medium	
Reliability*First* Corporation	URE2	1448	RFC2012010075	CIP-004-2	R2	Medium	
Reliability*First* Corporation	URE3	1448	RFC2012010076	CIP-004-2	R2	Medium	

[7] When NERC filed VRFs it originally assigned CIP-002-1 R3 a Medium VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on January 27, 2009, the Commission approved the modified High VRF. Therefore, the Medium VRF for CIP-002-1 R3 was in effect from June 18, 2007 until January 27, 2009 when the High VRF became effective.

[8] CIP-003-1 R1 has a "Medium" VRF; R1.1, R1.2 and R1.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-003-1 R1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req.	VRF	Total Penalty
Reliability*First* Corporation	URE1	1448	RFC201100966	CIP-004-1	R3	Lower[9]	
Reliability*First* Corporation	URE2	1448	RFC2011001278	CIP-004-1	R3	Lower	
Reliability*First* Corporation	URE3	1448	RFC2011001279	CIP-004-1	R3	Lower	
Reliability*First* Corporation	URE1	1448	RFC2011001280	CIP-004-1	R4	Lower[10]	
Reliability*First* Corporation	URE2	1448	RFC2011001281	CIP-004-1	R4	Lower	
Reliability*First* Corporation	URE3	1448	RFC2011001282	CIP-004-1	R4	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100967	CIP-005-1	R1	Medium[11]	
Reliability*First* Corporation	URE2	1448	RFC2011001178	CIP-005-1	R1	Medium	
Reliability*First* Corporation	URE3	1448	RFC2011001179	CIP-005-1	R1	Medium	
Reliability*First* Corporation	URE1	1448	RFC201100968	CIP-005-1	R2	Medium[12]	
Reliability*First* Corporation	URE2	1448	RFC2011001283	CIP-005-1	R2	Medium	
Reliability*First* Corporation	URE3	1448	RFC2011001284	CIP-005-1	R2	Medium	

[9] CIP-004-1 R3 has a "Medium" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-004-1 R3 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[10] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; R4.2 has a "Medium" VRF. When NERC filed VRFs, it originally assigned CIP-004-1 R4.2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-004-1 R4.2 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

[11] CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a "Medium" VRF; R1.6 has a "Lower" VRF.

[12] CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" VRF; R2.5 and its sub-requirements and R2.6 each have a "Lower" VRF.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req.	VRF	Total Penalty
Reliability*First* Corporation	URE1	1448	RFC201100969	CIP-005-1	R3	Medium	
Reliability*First* Corporation	URE1	1448	RFC201100970	CIP-005-1	R4	Medium	
Reliability*First* Corporation	URE1	1448	RFC201100971	CIP-005-1	R5	Lower	
Reliability*First* Corporation	URE2	1448	RFC2011001285	CIP-005-1	R5	Lower	
Reliability*First* Corporation	URE3	1448	RFC2011001286	CIP-005-1	R5	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100972	CIP-006-1	R1	Medium[13]	
Reliability*First* Corporation	URE2	1448	RFC2011001287	CIP-006-1	R1	Medium	
Reliability*First* Corporation	URE3	1448	RFC2011001288	CIP-006-1	R1	Medium	
Reliability*First* Corporation	URE1	1448	RFC201100973	CIP-007-1	R1	Medium[14]	
Reliability*First* Corporation	URE2	1448	RFC2011001289	CIP-007-1	R1	Medium	
Reliability*First* Corporation	URE3	1448	RFC2011001290	CIP-007-1	R1	Medium	
Reliability*First* Corporation	URE1	1448	RFC201000561	CIP-007-1	R2	Medium	
Reliability*First* Corporation	URE2	1448	RFC201000582	CIP-007-1	R2	Medium	
Reliability*First* Corporation	URE3	1448	RFC201000540	CIP-007-1	R2	Medium	
Reliability*First* Corporation	URE1	1448	RFC2012009913	CIP-007-1	R2	Medium	

[13] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; R1.7 and R1.8 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-006-1 R1.5 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on February 2, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-006-1 R1.5 was in effect from June 18, 2007 until February 2, 2009, when the "Medium" VRF became effective.

[14] CIP-007-1 R1 and R1.1 each have a "Medium" VRF; R1.2 and R1.3 each have a "Lower" VRF.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req.	VRF	Total Penalty
Reliability*First* Corporation	URE2	1448	RFC2012009914	CIP-007-1	R2	Medium	
Reliability*First* Corporation	URE3	1448	RFC2012009915	CIP-007-1	R2	Medium	
Reliability*First* Corporation	URE1	1448	RFC201100974	CIP-007-1	R3	Lower	
Reliability*First* Corporation	URE2	1448	RFC2011001291	CIP-007-1	R3	Lower	
Reliability*First* Corporation	URE3	1448	RFC2011001292	CIP-007-1	R3	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100975	CIP-007-1	R3	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100976	CIP-007-1	R4	Medium[15]	
Reliability*First* Corporation	URE2	1448	RFC2011001293	CIP-007-1	R4	Medium	
Reliability*First* Corporation	URE3	1448	RFC2011001294	CIP-007-1	R4	Medium	
Reliability*First* Corporation	URE1	1448	RFC201100977	CIP-007-1	R5	Lower	
Reliability*First* Corporation	URE2	1448	RFC2011001180	CIP-007-1	R5	Lower	
Reliability*First* Corporation	URE3	1448	RFC2011001181	CIP-007-1	R5	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100978	CIP-007-1	R5	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100979	CIP-007-1	R6	Lower	
Reliability*First* Corporation	URE2	1448	RFC2011001295	CIP-007-1	R6	Lower	
Reliability*First* Corporation	URE3	1448	RFC2011001296	CIP-007-1	R6	Lower	

[15] When NERC filed VRFs it originally assigned CIP-007-1 R4 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on February 2, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-007-1 R4 was in effect from June 18, 2007 until February 2, 2009, when the "Medium" VRF became effective.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req.	VRF	Total Penalty
Reliability*First* Corporation	URE1	1448	RFC201100981	CIP-007-1	R8	Lower[16]	
Reliability*First* Corporation	URE1	1448	RFC201100982	CIP-008-1	R1	Lower	
Reliability*First* Corporation	URE2	1448	RFC2011001182	CIP-008-1	R1	Lower	
Reliability*First* Corporation	URE3	1448	RFC2011001183	CIP-008-1	R1	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100983	CIP-009-1	R1	Medium	
Reliability*First* Corporation	URE2	1448	RFC2011001184	CIP-009-1	R1	Medium	
Reliability*First* Corporation	URE3	1448	RFC2011001185	CIP-009-1	R1	Medium	
Reliability*First* Corporation	URE1	1448	RFC201100984	CIP-009-1	R2	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100985	CIP-009-1	R3	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100986	CIP-009-1	R4	Lower	
Reliability*First* Corporation	URE2	1448	RFC2011001299	CIP-009-1	R4	Lower	
Reliability*First* Corporation	URE3	1448	RFC2011001300	CIP-009-1	R4	Lower	
Reliability*First* Corporation	URE1	1448	RFC201100987	CIP-009-1	R5	Lower	
Reliability*First* Corporation	URE2	1448	RFC2011001186	CIP-009-1	R5	Lower	
Reliability*First* Corporation	URE3	1448	RFC2011001187	CIP-009-1	R5	Lower	

Reliability*First* discovered the violations through the following mechanisms.

1. The UREs submitted a Self-Report to Reliability*First*, identifying violations of CIP-007-1 R2;[17]

[16] CIP-007-1 R8 and R8.1 each have a "Lower" VRF; R8.2, R8.3 and R8.4 each have a "Medium" VRF.
[17] These include the violations identified as RFC201000540, RFC201000561, and RFC201000582.

2. Immediately preceding URE1's Compliance Audit, URE1 submitted Self-Reports to Reliability*First* describing URE1's various instances of noncompliance with the CIP Standards;[18]

3. Reliability*First* conducted a Compliance Audit of URE1 (the URE1 Compliance Audit). During the URE1 Compliance Audit, Reliability*First* identified additional facts regarding many of the self-reported violations, as well as additional violations of the CIP Standards;[19]

4. URE2 and URE3 submitted Self-Reports to Reliability*First*, stating URE2 and URE3's noncompliance with more CIP Standards, but providing no information regarding the underlying facts of each violation. Reliability*First* requested additional information, which the UREs provided.[20] Reliability*First* worked collaboratively with the UREs to address their noncompliance with the CIP Reliability Standards. This included a compilation and analysis of information to better understand the scope of the noncompliance;

5. Reliability*First* conducted a Compliance Audit of URE2 and URE3 (Compliance Audit of URE2 and URE3). During the Compliance Audit of URE2 and URE3, Reliability*First* identified additional violations by URE2 and URE3.[21] However, Reliability*First* noted a marked improvement in the UREs' compliance with the CIP Reliability Standards;[22] and

---

[18] These include the violations identified as RFC201100962, RFC201100964, RFC201100965, RFC2011001280, RFC201100967, RFC201100969, RFC201100970, RFC201100972, RFC201100973, RFC201100974, RFC201100976, RFC201100977, RFC201100979, RFC201100981, RFC201100983, RFC201100984, RFC201100985, and RFC201100987.

[19] These include the violations identified as RFC201100957, RFC201100958, RFC201100959, RFC201100960, RFC201100961, RFC201100962, RFC201100963, RFC201100966, RFC2011001280, RFC201100967, RFC201100968, RFC201100971, RFC201100972, RFC201000561, RFC201100974, RFC201100975, RFC201100976, RFC201100977, RFC201100978, RFC201100979, RFC201100982, RFC201100983, RFC201100984, and RFC201100986.

[20] These include the violations identified as RFC2011001274, RFC2011001275, RFC2011001276, RFC2011001277, RFC2011001278, RFC2011001279, RFC2011001281, RFC2011001282, RFC201100967, RFC2011001178, RFC2011001179, RFC2011001283, RFC2011001284, RFC201100969, RFC201100971, RFC2011001285, RFC2011001286, RFC201100972, RFC2011001287, RFC2011001288, RFC2011001289, RFC2011001290, RFC2012009913, RFC2012009914, RFC2012009915, RFC201100974, RFC2011001291, RFC2011001292, RFC201100976, RFC2011001293, RFC2011001294, RFC2011001180, RFC2011001181, RFC2011001295, RFC2011001296, RFC2011001299, and RFC2011001300.

[21] Prior to the Compliance Audit of URE2 and URE3, the UREs notified Reliability*First* that numerous findings from the URE1 Compliance Audit also applied to URE2 and URE3, due to their shared compliance program. As a result, Reliability*First* narrowed and tailored the scope of the scheduled Compliance Audit of URE2 and URE3 to focus on ensuring that the UREs mitigated the violations. At the same time, the Reliability*First* Enforcement Department focused on continuing dialogue with, and requesting and analyzing information from, the UREs to understand and address the scope of their known noncompliance with the CIP Reliability Standards.

[22] These include the violations identified as RFC2011001281, RFC2011001282, RFC2011001178, RFC2011001179, RFC2011001285, RFC2011001286, RFC2011001180, RFC2011001181, RFC2011001182, RFC2011001183, RFC2011001184, RFC2011001185, RFC2011001186, and RFC2011001187. Reliability*First*'s observation regarding a marked improvement in the UREs' compliance with the CIP Reliability Standards is based on all the evidence received during its review of the UREs' compliance with the CIP Standards. By the time of the Compliance Audit of URE2 and URE3, Reliability*First* noted, *inter alia*, that many programs, processes, and procedures shared among all three entities were updated since the URE1 Audit. While

6. The UREs provided information to Reliability*First* identifying additional areas of noncompliance, which expanded the scope of certain identified violations.[23] Reliability*First* further identified additional violations.[24]

This Notice of Penalty lists the method of discovery and the specific facts of each area of noncompliance chronologically, by registered entity.

URE1's Violation of CIP-002-1 R1 (RFC201100957)

CIP-002-1 R1

The purpose statement of Reliability Standard CIP-002-1 provides in pertinent part: "Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment."

CIP-002-1 R1 provides in pertinent part:

> R1. Critical Asset Identification Method — The Responsible Entity[25] shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.
>
> > R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

* * * * *

[Footnote added.]

Reliability*First* found many violations during the Compliance Audit of URE2 and URE3, Reliability*First*'s analysis continued beyond the sheer quantity of violations.

[23] The Settlement Agreement states that the UREs provided information to Reliability*First* identifying additional areas of noncompliance.

[24] These include the violations identified as RFC201100959, RFC2011001274, RFC2011001275, RFC2011001276, RFC2011001277, RFC2012010075, RFC2012010076, RFC2011001278, RFC2011001279, RFC2011001281, RFC2011001282, RFC201100967, RFC2011001178, RFC2011001179, RFC2011001283, RFC2011001284, RFC201100969, RFC201100971, RFC2011001285, RFC2011001286, RFC201100972, RFC2011001287, RFC2011001288, RFC201100973, RFC2011001289, RFC2011001290, RFC2012009913, RFC2012009914, RFC2012009915, RFC201100974, RFC2011001291, RFC2011001292, RFC201100976, RFC2011001293, RFC2011001294, RFC201100977, RFC2011001180, RFC2011001181, RFC201100979, RFC2011001295, RFC2011001296, RFC2011001299, and RFC2011001300.

[25] Within the text of Standard CIP-002 – CIP-009, "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.

CIP-002-1 R1 has a Violation Risk Factor (VRF) of "Medium," and a "Severe" Violation Severity Level (VSL).

During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-002-1 R1 because URE1 failed to document the risk basis used by URE1's methodology to identify Critical Assets. Specifically, URE1's assessment methodology for determining Critical Assets did not explain how the described methodology was risk-based and did not document the risk basis used to create two of the eight criteria URE1's methodology utilized to identify Critical Assets.

URE1 violated CIP-002-1 R1 by failing to identify and document a risk-based assessment methodology (RBAM) to identify Critical Assets.

Reliability*First* determined the duration of the violation was from the date the Standard became mandatory and enforceable through when URE1 completed its Mitigation Plan.

Reliability*First* determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because the risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. Although URE1 failed to document the risk basis that it used to identify Critical Assets within its RBAM, URE1 did provide protections to ensure the identification and documentation of Critical Assets that support the reliable operation of the BPS. URE1 did identify a set of Critical Assets through the use of criteria; however, it failed to state that the criteria were risk-based. Furthermore, when URE1 mitigated the violation by documenting the risk bases within its RBAM, it did not alter its criteria or its designation of any Critical Assets.

URE1's Violation of CIP-002-1 R2 (RFC201100958)

CIP-002-1 R2

CIP-002-1 R2 provides: **"**Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary."

CIP-002-1 R2 has a "High" VRF and a "Severe" VSL. During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-002-1 R2 because URE1 failed to follow its process for identifying Critical Assets, as listed within its RBAM. Specifically, URE1's RBAM required URE1 to list all assets and facilities reviewed as possible Critical Assets, however, URE1 failed to list all substation Critical Assets. Instead, URE1's list of substation CCAs included a substation which was not included in URE1's list of

Critical Assets. Therefore, URE1 failed to determine its list of identified Critical Assets through an annual application of its RBAM.

URE1 violated CIP-002-1 R2 by failing to follow the procedures in its RBAM for identifying Critical Assets.

Reliability*First* determined the duration of the violation was from the date the Standard became mandatory and enforceable through when URE1 completed its Mitigation Plan.

Reliability*First* determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because the risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors.

While URE1 failed to follow its own process rigorously by failing to list all assets and facilities it had reviewed, it did complete the underlying review and determination of Critical Assets. Moreover, although URE1 excluded the substation at issue from the list of assets and facilities reviewed for Critical Assets, the substation did not contain Critical Assets.

URE1's Violation of CIP-002-1 R3 (RFC201100959)

CIP-002-1 R3
CIP-002-1 R3 provides:

> R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> > R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
> >
> > R3.2. The Cyber Asset uses a routable protocol within a control center; or,
> >
> > R3.3. The Cyber Asset is dial-up accessible.

CIP-002-1 R3 has a "High" VRF and a "Severe" VSL. During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-002-1 R3 because URE1 failed to develop its previous list of CCAs using the list of Critical Assets developed pursuant to CIP-002-1 R2. Specifically, URE1's previous list of CCAs included five substations that were not on its list of Critical Assets. Therefore, URE1 did not utilize the list of Critical Assets developed pursuant to CIP-002-1 R2 to develop a list of associated CCAs essential to the operation of the Critical Asset, as specified in CIP-002-1 R3.

In addition, during the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-002-1 R3. URE1's 2010 CCA Identification Procedure, Version 4 stated that the restriction of the identification of a Critical Cyber Asset to be a system that can "effect the loss of at least [XXX] mw [sic] of load." The procedure therefore instructed URE1 personnel to eliminate a category of Cyber Assets prior to identifying associated CCAs, rather than reviewing all Cyber Assets to identify associated CCAs, as specified in CIP-002-1 R3.

URE1 provided information to Reliability*First*, wherein it identified an additional area of URE1's noncompliance with CIP-002-1 R3. Specifically, during the course of implementing its Mitigation Plan and reviewing evidence of completion, the URE1 introduced an error into its list of CCAs when it updated the list. The URE1 failed to include two CCAs on its list of CCAs.

URE1 violated CIP-002-1 R3 by failing to develop its list of CCAs using its list of Critical Assets.

Reliability*First* determined the duration of the violation was from the date the Standard became mandatory and enforceable through when URE1 completed its Mitigation Plan.

Reliability*First* determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because the risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. While URE1 failed to follow its own process rigorously, the set of CCAs identified by URE1 was complete as the inclusion of the MW criteria in the application of URE1's methodology did not affect its list of identified CCAs.

Additionally, although URE1 erroneously failed to include two CCAs on its list of CCAs when it updated the list as noted above, it continued to provide each device with all the protections applicable to CCAs. Therefore, URE1 provided protections to CCAs associated with Critical Assets that support the reliable operation of the BPS.

URE1's Violation of CIP-002-1 R4 (RFC201100960)

CIP-002-1 R4
CIP-002-1 R4[26] provides:

R4. Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

CIP-002-1 R4 has a "Lower" VRF and a "Severe" VSL. During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-002-1 R4 because URE1 failed to keep a signed and dated record of the senior manager or delegate's approval of the null list of CCAs for four substations identified as Cyber Assets.

Additionally, during the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-002-1 R4 when URE1 failed to demonstrate that a senior manager or delegate annually approved the list of Critical Assets and the list of CCAs. Instead, URE1 submitted inconsistent evidence of approval for its Critical Asset list and its CCA list. Specifically, URE1 provided an approval sheet separately from each CCA list and Critical Asset list. Each approval sheet states its approval of a similar, but not identical, document title to the document requiring approval. Additionally, the approval dates for each Critical Asset list and each CCA list are inconsistent among the documents submitted by URE1 to Reliability*First*. Therefore, URE1 could not demonstrate annual approval of its CCA list or of its Critical Asset list.

Finally, during the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-002-2 R4 when URE1 failed to ensure that a senior manager or delegate annually approved a RBAM. Specifically, URE1's RBAM was not approved by the senior manager or delegate too late. CIP-002-2 became effective on April 1, 2010 and requires annual approval of the RBAM. Therefore, the RBAM should have been approved by April 1, 2010. Furthermore, the evidence demonstrating senior manager's late approval consists of an e-mail thread which shows a request for approval of a document contained within a zip file, but URE1 failed to provide a signature sheet evidencing the senior manager's approval.

[26] Versions 2 and 3 of CIP-002, R4 state, in pertinent part, "… [t]he senior manager or delegate(s) shall approve annually ***the risk-based assessment methodology***, the list of Critical Assets and the list of Critical Cyber Assets." (Emphasis added).

URE1 violated CIP-002-1 R4 when it failed to: (a) keep a signed and dated record of the senior manager or delegate's approval of the null list of CCAs; (b) demonstrate a senior manager or delegate annually approved the list of Critical Assets and the list of CCAs; and (c) ensure a senior manager or delegate annually approved a RBAM.

Reliability*First* determined the duration of the violation was from the date the Standard became mandatory and enforceable to when URE1 completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. This violation evidenced URE1 management's failure to review and approve necessary processes and procedures and overall lack of involvement in CIP compliance. The risk to the reliability of the BPS during the pendency of the violation was mitigated by several factors. URE1 represented that it conducted an annual assessment of its Critical Assets and CCAs, even though it failed to maintain documentation evidencing this annual assessment. Furthermore, when URE1 mitigated the violation by conducting and documenting the annual approval of each Critical Asset and CCA list, no additional Critical Assets or CCAs were identified. Therefore, URE1 provided some protections to ensure the identification and documentation of CCAs associated with Critical Assets that support the reliable operation of the BPS.

URE1's Violation of CIP-003-1 R1 (RFC201100961)

CIP-003-1 R1

The purpose statement of Reliability Standard CIP-003-1 provides in pertinent part: "Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-003-1 R1 provides:

> R1.Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:
>
> > R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
> >
> > R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

CIP-003-1 R1 has a "Medium" VRF and a "High" VSL. During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-003-1 R1 because, in several instances, URE1 failed to implement its cyber security policy. Specifically, URE1's cyber security policy required the physical security plan to include documentation of the Physical Security Perimeter (PSP), but URE1 failed to implement this provision of its cyber security policy. Furthermore, URE1's cyber security policy requires a CCA recovery plan, but URE1's recovery plan and the successor document do not include all the elements required by URE1's cyber security policy.

URE1 violated CIP-003-1 R1 by failing to implement its cyber security policy that represents management's commitment and ability to secure its CCAs.

Reliability*First* determined the duration of the violation was from the date the Standard became mandatory and enforceable to when URE1 completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-003-1 R1 has the potential to affect the reliable operation of the bulk power system by decreasing the likelihood that a Responsible Entity will have proper security management controls in place. A risk to the BPS is present when an entity partially implements its cyber security policy. Partial implementation of a cyber security policy increases the likelihood of security gaps or unnecessary access points to the critical infrastructure of the BPS and weakens an entity's security posture. Furthermore, the cyber security policy evidences management's expectation for security and adherence to regulatory requirements. Partial implementation of the cyber security policy indicates that these requirements are not being met, which has the potential to impact the reliability of the BPS. The risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. URE1 represented that the specific instances of URE1's partial implementation of the cyber security policy consisted of inconsistent cross-referencing of the cyber security policy and related documents and did not relate to substantive noncompliance with the policy or any inadequacy or the failure of any cyber security protections. Therefore, URE1's partial implementation of the cyber security policy did not pose a serious or substantial risk to the security of its Critical Assets.

URE1's Violation of CIP-003-1 R5 (RFC201100962)

CIP-003-1 R5
CIP-003-1 R5 provides:

> R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
>
> R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
>
> R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.
>
> R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.
>
> R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
>
> R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

CIP-003-1 R5 has a "Lower" VRF and a "High" VSL.

URE1 submitted a Self-Report in advance of URE1's Compliance Audit to Reliability*First*, identifying a violation of CIP-003-1 R5. Within the Self-Report, URE1 stated that it failed to implement its program for managing access to protected CCA information. Specifically, URE1 failed to create, maintain, and annually verify a list of designated personnel who are responsible for authorizing logical or physical access to protected information, as specified in CIP-003-1 R5.1. Additionally, URE1 failed to annually review the access privileges to protected information, as specified in CIP-003-1 R5.2. Finally, URE1 failed to annually assess and document the process for controlling access privileges to protected information, as specified in CIP-003-1 R5.3.

Subsequently, during the URE1 Compliance Audit, Reliability*First* reviewed additional facts related to URE1's compliance with CIP-003-1 R5. Reliability*First* determined that URE1 failed to confirm that

access privileges for substation personnel were correct and that they corresponded with URE1's needs and appropriate personnel roles and responsibilities. URE1 has criteria which define access rights based on specific roles and responsibilities, and separately lists the individuals with access to CCA information; however, no document links the URE1 personnel list to the list of defined and approved roles and responsibilities. Therefore, URE1 could not confirm that access privileges for substation personnel were correct and that they corresponded with URE1's needs and appropriate personnel roles and responsibilities, as specified in CIP-003-1 R5.2.

During the URE1 Compliance Audit, Reliability*First* also discovered that URE1 failed to document activities to confirm that the access privileges for Emergency Management System (EMS) personnel were correct and that they corresponded with URE1's needs and appropriate personnel roles and responsibilities, as specified in CIP-003-1 R5.2.

Finally, during the URE1 Compliance Audit Reliability*First* discovered that URE1 failed to document that it annually assessed its processes for controlling access privileges to protected information for the URE1 substations and the URE1 EMS, as specified in CIP-003-1 R5.3.

URE1 violated CIP-003-1 R5 by failing to implement a program for managing access to protected CCA information.

Reliability*First* determined the duration of the violation was from the date the Standard became mandatory and enforceable to when URE1 completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a risk to the BPS is present when a Responsible Entity permits the opportunity for unauthorized access to CCA information. Unauthorized access could lead to disruptive acts, up to and including the loss of a substation. Without the implementation of correct processes to control access to protected information, a Responsible Entity cannot be certain that protected information is properly secured.

Reliability*First* considered the fact that the risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. URE1 represented that it limited access to CCA information to personnel with a need to know and ensured this protection through the use of technical restrictions, such as access control lists (ACLs) in its active directory. These ACLs specify access levels for each user based on the organization's needs and the user's roles and responsibilities. URE1 represented that it maintained awareness of those limited personnel who were responsible for authorizing access, even though it failed to maintain this information in a formal list that could be verified annually.

URE1 represented that it reviewed the processes for controlling access privileges to protected information, even though it failed to formally document an annual assessment of the control processes. Additionally, URE1 confirmed through a subsequent review that access privileges correspond with URE1's needs and appropriate personnel roles and responsibilities.

Furthermore, URE1's technical controls for maintaining CCAs were in place at the time of the violation. Specifically, URE1 has a private network for its Critical Asset substations that isolates Critical Asset substation data traffic from all other bulk electric and distribution traffic and is isolated from URE1's Corporate IT network by firewalls. Additionally, URE1 controls remote access to all Critical Asset substations through Parent Company's Substation access control system, which utilizes two-factor authentication. Finally, URE1 controls access privileges to ensure that only those individuals who meet the requirements listed within the CIP Reliability Standards are permitted access to protected information.

The UREs' Violations of CIP-003-1 R6 (RFC201100963, RFC2011001274, and RFC2011001275)

CIP-003-1 R6
CIP-003-1 R6 provides:

> R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

CIP-003-1 R6 has a "Lower" VRF and a "High" VSL.[27] During the URE1 Compliance Audit, Reliability*First* discovered that URE1 failed to establish and document a process for configuration management for CCA hardware or software or supporting configuration management activities in the Change Control Process of the Security Services Change Control and Configuration Management Plan, as specified in CIP-003-1 R6.

Additionally, during the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-003-1 R6 because Reliability*First* determined, based on evidence reviewed, that URE1 failed to implement supporting configuration management activities to identify, control and document all changes to

[27] The settlement agreement states the VSL for this violation is Moderate. The UREs failed to establish and document a configuration management process. On further review, Reliability*First* believes the VSL should be "High." Reliability*First* also notes that this change would not have affected the resolution of the alleged violations.

hardware and software components of CCAs pursuant to the change control process. Specifically, URE1 failed to establish and document its process of change control in the removal of the legacy EMS and the subsequent replacement with its new EMS, as specified in CIP-003-1 R6. URE1 confirmed that it did not create a change control form for this replacement.

The UREs provided additional information to Reliability*First* identifying URE2 and URE3's noncompliance with CIP-003-1 R6. Specifically, URE2 and URE3 failed to establish and document a process for configuration management for adding, modifying, replacing, or removing CCA hardware or software, and for implementing supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of CCAs.

The UREs violated CIP-003-1 R6 by failing to establish and to document a process for configuration management for adding, modifying, replacing, or removing CCA hardware or software, and implementing supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of CCAs. Additionally, URE1 violated CIP-003-1 R6 by failing to implement supporting configuration management activities to identify, control and document all changes to hardware and software components of CCAs.

Reliability*First* determined the duration of URE1's violation was from the date the Standard became mandatory and enforceable to the date URE1 completed the Mitigation Plan. The duration of URE2 and URE3's violations of CIP-003-1, R6 was from the date the Standard became mandatory and enforceable to when URE2 and URE3 completed the mitigating activities necessary to remedy their violations.

Reliability*First* determined that these violations posed a serious and substantial risk to the reliability of the BPS. A risk to the BPS is present when minimum security management controls are not in place to protect Critical Assets. In particular, configuration management ensures the network environment is properly managed with consistent versions and settings so that the environment remains secure. Insufficient implementation and support of configuration management can introduce unwanted security vulnerabilities and unauthorized access points and can impact the availability of critical systems, up to and including the BPS.

In considering the risk posed by the UREs' violations of CIP-003-1 R6, Reliability*First* also considered the fact that the risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. Although the UREs did not have a configuration management procedure, each of the UREs has an established change control process. Additionally, although URE1 did not document its change from the legacy EMS system to the new EMS through the use of a change control form, URE1 represented that it documented and controlled the

changes associated with the EMS replacement through other processes. Specifically, the legacy EMS installation and commissioning process included functionality testing to ensure that there was no adverse effect on cyber security controls, that cyber security baselines were established, and that the EMS Cyber Assets were afforded protective measures such as access control, user account management, and change management controls. Therefore, the UREs did provide certain security management controls to protect Critical Assets.

The UREs' Violations of CIP-004-1 R1 (RFC201100964, RFC2011001276, and RFC2011001277)

CIP-004-1 R1

The purpose statement of 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. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-004-1 R1[28] provides:

> R1. Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:
>
> - Direct communications (e.g., emails, memos, computer based training, etc.);
> - Indirect communications (e.g., posters, intranet, brochures, etc.);
> - Management support and reinforcement (e.g., presentations, meetings, etc.).

CIP-004-1 R1 has a "Lower" VRF and a "Severe" VSL.

URE1 submitted a Self-Report to Reliability*First*, identifying a violation of CIP-004-1 R1. Six months later, the UREs provided additional information to Reliability*First*, stating that the information listed in URE1's Self-Report was also applicable to URE2 and URE3. Within the Self-Report and the additional information, the UREs stated that they had no formal process to ensure that vendors and contractors

[28] Versions 2 and 3 of CIP-004, R1 state, in pertinent part, "[t]he Responsible Entity shall establish, document, ***implement***, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices..." (Emphasis added).

with remote access to CCAs receive quarterly security awareness reinforcements, pursuant to CIP-004-1 R1.

The UREs violated CIP-004-1 R1 by failing to establish, maintain, and document a security awareness program to ensure vendors and contractors having authorized cyber access to CCAs receive reinforcement in sound security practices on at least a quarterly basis.

The duration of the violations was from the date the Standard became mandatory and enforceable to the date the UREs completed their Mitigation Plan.

Reliability*First* determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS because the risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. The UREs have a security awareness program for employees and provide reinforcement to on-site contractors and vendors. Additionally, all personnel with cyber access to CCAs received annual cyber security training and also received the required quarterly reinforcement in sound security practices during onsite visits to a Parent Company office or upon attempted access of the UREs' network. As a result, while the security awareness program did not ensure that off-site contractors received the required quarterly security reinforcements, the UREs did not have any off-site contractors with authorized cyber or unescorted physical access to CCAs. Therefore, the UREs' provision of security awareness training reduced the risk of the violations.

The UREs' Violations of CIP-004-2 R2 (RFC201100965, RFC2012010075, and RFC2012010076)

CIP-004-2 R2
CIP-004-2 R2 provides:

> R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.
>
> > R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

> R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, 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.

CIP-004-2 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 are each assigned a "Lower" VRF and CIP-004-2 R2.1, R2.2 and R2.2.4 are each assigned a "Medium" VRF, the facts of the violations relate to CIP-004-2 R2.1, which has a VRF of "Medium" and a "Severe" VSL. URE1 submitted a Self-Report to Reliability*First*, identifying a possible violation of CIP-004-2 R2. Twelve days later, the UREs provided additional information to Reliability*First*, stating that the information listed in URE1's Self-Report was also applicable to URE2 and URE3. Within the Self-Report and additional information submitted, the UREs stated that they granted authorized unescorted physical access to CCAs to an employee without providing the employee with physical security training prior to granting access.

The UREs violated CIP-004-2 R2 by failing to ensure that all personnel having authorized unescorted physical access to CCAs were trained prior to their being granted such access, pursuant to their cyber security training programs.

Reliability*First* determined the duration of these violations was from the date that the UREs were required to comply with CIP-004-2 R2, to the date on which the UREs revoked the employee's physical access to CCAs. The UREs completed their Mitigation Plans a little over two years after Reliability*First* determined the duration of the violations.[29]

Reliability*First* determined that these violations posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because the risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. The violations were relatively short in duration and involved one employee. This employee was a trusted

[29] For these violations, the UREs submitted two mitigation plans (one of which included URE1's mitigating activities, RFCMIT007197, and one to include URE2 and URE3's mitigating activities, RFCMIT007237).

manager who had received some of the required cyber security training, as well as a personnel risk assessment (PRA) that had identified no issues. Furthermore, the employee did not attempt physical access to CCAs. Additionally, the UREs have security awareness programs in place for employees, which include updates and training reinforcement for on-site contractors and vendors. Therefore, the UREs had measures in place to reduce the risk of the violations.

The UREs' Violations of CIP-004-1 R3 (RFC201100966, RFC2011001278 RFC2011001279)

CIP-004-1 R3
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:
>
> * * * * *
>
> R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

CIP-004-1 R3 has a "Medium" VRF; R3.1, R3.2 and R3.3 each have a "Lower" VRF. The facts of the violations relate to CIP-004-1 R3.2, which has a VRF of "Lower" and a "High" VSL. During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-004-1 R3 by concluding that URE1's documented PRA program does not contain a provision requiring URE1 to conduct PRAs for cause, as specified in CIP-004-1 R3.2.

Later, the UREs provided information to Reliability*First*, wherein they identified URE2 and URE3's noncompliance with CIP-004-1 R3. Specifically, URE2 and URE3's PRA program did not contain a provision requiring them to conduct PRAs for cause, as specified in CIP-004-1 R3.2.

The UREs violated CIP-004-1 R3 by failing to include provisions within their PRA programs requiring them to update PRAs for cause.

Reliability*First* determined the duration of these violations was from when the Standard became mandatory and enforceable to the date the UREs updated their PRA programs to remediate the violations and completed their Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because the risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. The UREs' PRA programs contained all necessary elements except for the provision to update PRAs for cause. The UREs had an informal policy to update PRAs for cause. The individuals responsible for conducting PRAs were aware of this policy. Moreover, the UREs confirmed that they experienced no instances invoking the need to conduct a PRA for cause during the time period of the violations. Therefore, the UREs provided certain safeguards to protect their CCAs against any harmful or unwanted access.

The UREs' Violations of CIP-004-1 R4 (RFC2011001280, RFC2011001281 RFC2011001282)

CIP-004-1 R4

CIP-004-1 R4 provides:

> 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 and R4.1 each have a VRF of "Lower" R4.2 has a "Medium" VRF. Applying the facts and circumstances of this violation, ReliabilityFirst determined a "Lower" VRF and a "Severe" VSL was appropriate.

URE1 submitted a Self-Report to ReliabilityFirst, identifying a possible violation of CIP-004-1 R4. Within the Self-Report, URE1 stated that it documented that it had granted an individual cyber access rights, but URE1 had not actually granted such access rights. Therefore, URE1 failed to maintain its lists of personnel with authorized cyber or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs, as specified by CIP-004-1 R4.

Within the Self-Report, URE1 also stated that it granted an employee authorized cyber access to Parent Company's access control system, but it failed to update its access lists within seven calendar days of this change, as specified by CIP-004-1 R4.1.

During the URE1 Compliance Audit, Reliability*First* discovered additional areas of URE1's noncompliance with CIP-004-1 R4. Specifically, Reliability*First* examined URE1's quarterly review and discovered that URE1 failed to conduct this quarterly review. Therefore, Reliability*First* determined that URE1 extended its review of the lists of its personnel who have authorized cyber or authorized unescorted physical access to CCAs beyond the quarterly basis specified by CIP-004-1 R4.1.

During the Compliance Audit of URE2 and URE3, Reliability*First* discovered additional areas of URE2 and URE3's noncompliance with CIP-004-1 R4. Specifically, URE2 and URE3 failed to perform quarterly reviews of the lists of their personnel who have authorized cyber or authorized unescorted physical access to CCAs as specified by CIP-004-1 R4.1.

The UREs provided additional information to Reliability*First*, wherein they identified additional areas of URE2 and URE3's noncompliance with CIP-004-1 R4. Specifically, URE2 and URE3 had granted access to an individual, but failed to document this access on their access lists, as specified by CIP-004-1 R4. Additionally, URE2 and URE3 failed to revoke access within seven calendar days for one employee who no longer required such access, as specified by CIP-004-1 R4.2.

Finally, the UREs provided additional information to Reliability*First*, wherein they identified additional areas of URE2 and URE3's noncompliance with CIP-004-1 R4. Specifically, URE2 and URE3 failed to document specific access rights of employees with access to CCAs. URE2 and URE3's procedures require that they document the permissions, roles, and responsibilities of employees with access to CCAs; however, the terminology utilized in the procedure and the user access list were inconsistent and did not adequately describe the specific access rights of employees with access to CCAs, as specified in CIP-004-1 R4.

The UREs violated CIP-004-1 R4 by failing to: (a) maintain their access lists for personnel with access to CCAs; (b) update access lists within seven calendar days of any change; and (c) perform quarterly reviews of the lists of their personnel who have access to CCAs. Reliability*First* also alleges that URE2 and URE3 violated CIP-004-1 R4 by failing to revoke authorized cyber or authorized unescorted physical access to CCAs within seven calendar days for personnel who no longer require such access to CCAs.

Reliability*First* determined the duration of the violations was from when the Standard became mandatory and enforceable to when the UREs completed their Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-004-1 R4 has the potential to affect the reliable operation of the BPS by providing the opportunity for personnel, that a Responsible Entity determined should no longer have access to CCAs, to still have access. This continued access could result in harm to the integrity of the CCAs or the reliability of the BPS as a result of actions by an individual who should no longer have physical or electronic access to CCAs. The risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. The violations involved a small number of individuals, namely four employees with functions at both URE2 and URE3 and two URE1 employees. The time period during which each access list was incorrect was relatively short in duration. The UREs conducted PRAs for five of the six individuals involved in the violations before those individuals were granted access. These five PRAs resulted in no negative findings. The UREs did not perform a PRA on the sixth employee, who retired one month after the effective date of CIP-004-1 R4, at which time the UREs instead revoked access. Additionally, the UREs provided annual cyber security training to each of the individuals involved in the violations. The UREs also represented that they experienced no unauthorized cyber or physical access attempts from any of the individuals involved in the violations.

Furthermore, the UREs have procedures in place governing authorized cyber and unescorted physical access to CCAs, in addition to a security awareness program. Finally, the UREs afforded their Cyber Assets with other technical protective measures to minimize threats and vulnerabilities, including implementing user and system activity logging and monitoring.

The UREs' Violations of CIP-005-1 R1 (RFC201100967, RFC2011001178, RFC2011001179)

CIP-005-1 R1

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

CIP-005-1 R1 provides, in pertinent part:

> 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).

* * * * *

> R1.4. 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, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a "Medium" VRF; R1.6 has a "Lower" VRF. Reliability*First* determined that the facts and circumstances of each of these violations warranted a "Medium" VRF and a "High" VSL. URE1 submitted a Self-Report to Reliability*First*, identifying a violation of CIP-005-1 R1. Six months later, the UREs provided additional information to Reliability*First*, stating that the information listed in URE1's Self-Report was also applicable to URE2 and URE3. Within the Self-Report and the additional information, the UREs identified their failure to provide the protections identified in CIP-005-1 R1.5 to several Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter (ESP).[30] Specifically, the UREs failed to: (a) ensure that one application displayed an appropriate use banner on the user screen upon all interactive access attempts, where technically feasible, as specified in CIP-005-1 R2; (b) ensure that significant changes to nineteen Cyber Asset devices did not adversely affect existing cyber security controls on the devices, as specified in CIP-007-1 R1; and (c) implement technical and procedural controls to enforce access authentication of, and accountability for, all user activity and to minimize the risk of unauthorized system access for service accounts, which are shared accounts, as specified in CIP-007-1 R5.

[30] URE1 also provided information to Reliability*First* concerning URE1's failure to afford Cyber Assets used in the access control and monitoring of the ESP with the protective measures specified in CIP-007-1 R8; CIP-009-1 R2; and CIP-009-1 R5. Reliability*First* reviewed the information submitted by URE1 and determined that URE1 had resolved each of these areas of noncompliance as documented in a previous settlement agreement. Therefore, Reliability*First* did not incorporate the facts related to URE1's noncompliance with CIP-007-1 R8; CIP-009-1 R2; and CIP-009-1 R5 within the violation of CIP-005-1 R1.

Within the Self-Report, URE1 also stated that it failed to submit the correct device count in two Technical Feasibility Exception (TFE) requests for devices used in the access control and monitoring of ESPs. In the first TFE, URE1 failed to include one of the firewalls used in the access control and monitoring of an ESP for devices that could not support anti-malware tools, as specified in CIP-007-1 R4, and failed to previously disclose this issue to Reliability*First* through a TFE. In the second TFE, URE1 failed to include a firewall on the TFE relating to the device's inability to implement technical controls that require the use of passwords consisting of a combination of alpha, numeric, and "special" characters for Cyber Assets that monitor and control access to ESPs, as specified in CIP-007-1 R5.3, and failed to previously disclose this issue to Reliability*First* through a TFE.

Within the Self-Report, URE1 also stated its failure to maintain accurate documentation of one ESP, as required under CIP-005-1 R1.6. Specifically, URE1 incorrectly included a firewall on a diagram of the emergency backup system (EBS) ESP.

Subsequently, during the URE1 Compliance Audit, Reliability*First* discovered that URE1 failed to afford the protective measures specified in CIP-007-1 R5.2.1 to a Critical Asset used in the access control and monitoring of the ESP. Specifically, URE1 failed to change the default password for an enabled default guest account on a Critical Asset located at a substation. Therefore, the asset was not afforded the protections required in CIP-007-1 R5.2.1, as specified by CIP-005-1 R1.5. The UREs provided additional information to Reliability*First*, stating that the information related to URE1's failure to change the default password for an enabled default guest account also revealed noncompliance by URE2 and URE3.

The UREs provided further information to Reliability*First*, wherein they disclosed additional instances of the UREs' noncompliance with CIP-005-1 R1. Specifically, the UREs stated that they failed to provide the following protections to Cyber Assets used in the access control and monitoring of the ESP: (a) enable only ports and services required for operations and for monitoring Cyber Assets within the ESP at all access points to the ESP, as specified in CIP-005-1 R2.2; (b) implement security patches for two Cyber Assets and hardware patches for one Cyber Asset used in the access control and monitoring of the ESP; (c) document compensating measures to mitigate the risk of exposure or acceptance of risk, as specified in CIP-007-1 R3; and (d) implement technical controls that require the use of passwords consisting of six characters, annual changing, and a combination of alpha, numeric, and "special" characters for Cyber Assets that monitor and control access to ESPs, as specified in CIP-007-1 R5.3.

The UREs provided information to Reliability*First*, wherein they identified additional areas of URE1's noncompliance with CIP-005-1 R1. Specifically, during the course of implementing the Mitigation Plan and reviewing the evidence of milestone completion, the UREs determined that URE1 failed to apply appropriate use banners, as specified in CIP-005-1 R2.6, on the two monitoring systems located within

the ESP of URE1's EMS and EBS. In addition, the UREs determined that URE1 removed three access points from URE1's EMS without resetting them to their factory default settings before sending the devices back to the vendor. Therefore, URE1 failed to: (a) destroy or erase the data storage media, prior to disposing of Cyber Assets used in the access control and monitoring of the ESP to prevent unauthorized retrieval of sensitive cyber security or reliability data, as specified in CIP-007-1 R7 and (b) implement its process of change control, as specified in CIP-003-1 R6.

During the Compliance Audit of URE2 and URE3, Reliability*First* discovered that URE2 and URE3 failed to properly document all access points to their ESPs, as required by CIP-005-1 R1.6. Specifically, URE2 and URE3 listed two devices as access control and monitoring devices, when in fact these devices are access points to the ESP. Additionally, URE2 and URE3 defined two additional devices as CCAs, when these devices are access points to the ESP.

The UREs disclosed additional areas of URE2 and URE3's noncompliance with CIP-005-1 R1. Specifically, the UREs stated that URE2 and URE3 failed to accurately reflect the infrastructure of their EMS network on the EMS ESP drawings, as required by CIP-005-1 R1.6.

Additionally, URE2 and URE3 identified their failure to provide the protections identified in CIP-005-1 R1.5 to several Cyber Assets used in the access control and monitoring of the ESP. Specifically, the URE2 and URE3 failed to: (a) document that the testing of firewalls used in the access control and monitoring of the ESP is performed in a manner that reflects the production environment, as specified in CIP-007-1 R1.2; (b) enable only those ports and services required for normal and emergency operations for 25 Cyber Assets that monitor and control access to the ESPs, as specified in CIP-007-1 R2; (c) implement security patches for two operating systems used in the access control and monitoring of the ESP and document compensating measures to mitigate the risk exposure or acceptance of risk, as specified in CIP-007-1 R3; (d) implement technical controls that require the use of passwords consisting of a combination of alpha, numeric, and "special" characters for 25 Cyber Assets that monitor and control access to ESPs, as specified in CIP-007-1 R5.3; and (e) create recovery plans for Cyber Assets used in the access control and monitoring of the ESPs, as specified in CIP-009-1 R1.

All of the UREs provided additional information to Reliability*First* regarding their noncompliance with CIP-005-1 R1. Specifically, upon completing their Cyber Vulnerability Assessments, the UREs discovered that several CCAs included on their substation CCA lists did not match their respective ESP drawings, as specified by CIP-005-1 R1.6.

Finally, the UREs provided additional information to Reliability*First* regarding their noncompliance with CIP-005-1 R1.4. Specifically, during the course of implementing their Mitigation Plans for CIP-007-1 R3

and CIP-007-1 R4, the UREs determined that the field maintenance laptops addressed by these Mitigation Plans should be identified on their ESP diagrams as non-critical Cyber Assets within a defined ESP, as specified by CIP-005-1 R1.4.

The UREs violated CIP-005-1 R1 by failing to: (a) afford the protective measures specified in each of the CIP Reliability Standards listed in CIP-005-1 R1.5 to Cyber Assets used in the access control and monitoring of the ESP; and (b) maintain documentation of ESPs, all interconnected Critical and non-critical Cyber Assets within the ESP(s), all electronic access points to the ESP(s), and the Cyber Assets deployed for the access control and monitoring of these access points.

Reliability*First* determined the duration of these violations was from when the Standard became mandatory and enforceable to when the UREs are due to complete their Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. A violation of CIP-005-1 R1 has the potential to affect the reliable operation of the BPS by providing the opportunity for cyber intrusions to occur on CCAs located outside an established ESP. An ESP aids in the detection and prevention of cyber intrusions that could harm the integrity of a CCA or the reliability of the BPS. The risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. The UREs' violations of CIP-005-1 R1.4 and R1.6 were documentation deficiencies related to their incorrect ESP drawings. The UREs left no device unprotected as a result of this error. Additionally, the UREs established and implemented procedures to ensure that they controlled electronic access at all electronic access points to their ESPs. The UREs installed, implemented, and documented a multi-tiered Access Control Solution, which protected both their CCAs within their substations and the protection devices used to protect those locations, including certain devices. Furthermore, the UREs determined that even though their ESP diagrams for substations were not properly documented, the UREs accounted for these devices at these substations on the CCAs List, and afforded them the protections required under CIP-005-1 R1.

The risk posed by the UREs' violations of CIP-005-1 R1.6 was additionally reduced by the fact that the UREs deployed firewalls and Parent Company's access control system. Parent Company's access control system securely communicates with Parent Company's server, which authenticates those seeking access to the UREs' substations as well as its discrete devices, such as protective relays, Remote Terminal Units (RTUs), firewalls, and network switches. The UREs also developed lists for the access control system and ensured that only personnel who have a functional need to access the devices are granted access.

URE1 also failed to provide accurate TFE information regarding CIP-007-1 R4 and R5.3 compensating measures. In both instances, URE1 provided the firewall with all protections required under the previously-filed TFEs. The risk of the UREs' failure to change the default password as specified by CIP-007, R5.2.1, was lessened by the fact that access to the asset was restricted by the Parent Company's access control system and the substation firewall. The risk posed by the UREs's failure to afford the protective measures specified in CIP-005-1 R2.2 was mitigated by the fact that UREs' server build processes and standard operating procedures were designed to limit open ports and services to those which are required according to vendor specification. The UREs' policy is to deny access to Cyber Assets by default, so if a port was not shut down, any unauthorized access attempts would be identified. Additionally, security controls are in place for these assets, including configuration management, change controls, patch management, malware protection, electronic and physical access controls, and system security monitoring.

The risk posed by the UREs failure to afford the protective measures specified in CIP-007-1 R1 was mitigated by the fact that the UREs had in place test procedures that they implemented when making significant changes to these servers. The UREs' test procedures confirmed that existing Cyber Assets were not adversely affected and that they continued to operate and perform their security functions after a significant change.

The risk posed by the UREs 'failure to afford the protective measures specified in CIP-007-1 R3 was mitigated by the fact that the UREs evaluated and applied patches released by the manufacturer of the server, although one patch was not evaluated within the required 30-day period. Further, server patches are cumulative, so application of any patch release would update any patches that may not have been previously installed. Although the UREs failed to document their review of patches for the server application and for the database, the UREs later confirmed that no security patches had been released during the noncompliance period.

The risk posed by the UREs' failure to afford the protective measures specified in CIP-007-1 R5.2 was mitigated by the fact that the default accounts on the devices are not utilized for user login. Furthermore, these passwords do not provide access to any CCAs. Additionally, the devices are not Cyber Assets, and none of the devices are located within an ESP. The electronic access monitoring and control devices are located within a PSP, which controlled physical access to the devices. The physical access authorizing and logging devices are provided the physical protections required by CIP-006-1 R3.

The risk posed by the UREs' failure to afford the protective measures specified in CIP-007-1 R5.3 was mitigated by the fact that the UREs have procedural controls in place, requiring that all personnel use passwords that meet the complexity requirements of CIP-007-1 R5.3. The UREs have technical controls in place that enforce password length and annual password changes for passwords. The UREs are in

the process of submitting TFEs to Reliability*First* to reflect the fact that the password complexity rules, although they contain stringent requirements, do not correspond exactly to the requirements specified in CIP-007-1 R5.3. For the application, the devices, and the application, the UREs also implemented procedural controls. The UREs additionally limit physical and electronic access to these applications and devices.

The risk posed by URE2's and URE3's failure to afford the protective measures specified in CIP-007-1 R1 was mitigated by the fact that URE2 and URE3 represented that the violations relate only to the lack of a firewall test environment, which constitutes a small subset of EMS devices, and furthermore only affected five EMS firewalls. URE2 and URE3 also represented that they tested a majority of Cyber Assets prior to production.

The risk posed by the URE2's and URE3's failure to afford the protective measures specified in CIP-007-1 R2 and R3 was mitigated by the fact that URE2 and URE3 have a number of other protective measures in place to ensure that access to the ESP and the Cyber Assets located within the ESP are secured and monitored. Remote access to all ESPs and the Cyber Assets located within those ESPs is controlled by Parent Company's servers that validate all users' access. The Servers and two-factor authentication provide the only means of external access to the EMS.

The risk posed by the URE2's and URE3's failure to afford the protective measures specified in CIP-007-1 R5.3 was mitigated by the fact that URE2 and URE3 had a procedural control in place that required that all personnel use passwords that meet the requirements of CIP-007-1 R5.3.

The risk posed by the URE2's and URE3's failure to afford the protective measures specified in CIP-009-1 R1 was mitigated by the fact that URE2 and URE3's Cyber Assets that monitor and/or control access to ESPs are afforded protective measures that protect against misuse and provide URE2 and URE3 with situational awareness of these Cyber Assets. These protective measures include locating these Cyber Assets within a PSP and providing electronic access control, anti-virus software where technically feasible, and user and system activity logging and monitoring.

The risk posed by the URE1's failure to afford the protective measures specified in CIP-005-1 R2.6 was mitigated by the fact that all other Cyber Assets within the URE1 EMS and EBS ESPs display appropriate use banners; all personnel with access rights have PRAs on file and have successfully completed cyber security training; and URE1 has provided other protections, including restricting physical and electronic access, utilizing firewalls that deny access for any access that is not required for normal and emergency operations, and requiring personnel to monitor for attempts at or actual unauthorized access.

The risk posed by the URE1's failure to afford the protective measures specified in CIP-003-1 R6 and CIP-007-1 R7 was mitigated by the fact that the three access points do not have hard drives and the

only information that can be discovered from these devices is limited to the host name, simple network management protocol settings, IP address of the device itself, and the IP address of the front-end processors.

The UREs' Violations of CIP-005-1 R2 (RFC201100968, RFC2011001283, and RFC2011001284)

CIP-005-1 R2

CIP-005-1 R2 provides, in pertinent part:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> * * * * *
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
>
> * * * * *
>
> 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" and a "Severe" VSL. During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-005-1 R2 by concluding that URE1 failed to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP. Specifically, URE1 failed to provide evidence demonstrating that it only enabled ports for devices (serial servers) and the EMS and EBS ESP firewalls that were required for operations and for monitoring Cyber Assets within the ESP, as specified in CIP-005-1 R2.2. URE1 also failed to provide a list of open ports and services or an explanation of the necessity for the open ports and services.

During the URE1 Compliance Audit, Reliability*First* also discovered that URE1 failed to display an appropriate use banner on the user screen of an electronic access control device during interactive access attempts, as specified in CIP-005-1 R2.6.

The UREs provided additional information to Reliability*First*, wherein they disclosed URE2 and URE3's noncompliance with CIP-005-1 R2. Specifically, URE2 and URE3 failed to display an appropriate use banner on the user screen of electronic access control devices upon all interactive access attempts, as specified in CIP-005-1 R2.6. Additionally, URE2 and URE3 determined that their EMS firewalls did not support an appropriate use banner for certain logins, and that URE2 and URE3 previously failed to file a TFE for devices that were technically unable to comply with CIP-005-1 R2.6.

The UREs violated CIP-005-1 R2 by failing to ensure electronic access control devices display an appropriate use banner on the user screen upon all interactive access attempts. URE1 also violated CIP-005-1 R2 by failing to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP at all access points to the ESP.

Reliability*First* determined the duration of URE2 and URE3's violations of CIP-005-1 R2 was from when the Standard became mandatory and enforceable to when URE2 and URE3 completed the mitigating activities necessary to remedy the violation. The duration of URE1's violation of CIP-005-1 R2 was from when the Standard became mandatory and enforceable to when URE1 completed the mitigating activities necessary to remedy its violation.[31]

Reliability*First* determined that these violations posed a moderate and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-005-1 R2 has the potential to affect the reliable operation of the BPS by providing 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. The risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. The UREs had an appropriate use banner configured on their access control system, through which identification, authentication, and authorization must occur before a user may access certain assetsor firewalls. Consequently, all URE1 users were required to acknowledge an appropriate use banner before they were able to gain access to URE1's assets or firewalls.

Furthermore, the UREs provide technical controls to limit unauthorized access to their EMS. Specifically, the Cyber Assets within the EMS ESP were located within an established PSP and were afforded other protective measures, such as physical and cyber access controls, user account controls,

[31] The certification and verification documents state that the Mitigation Plan was completed for all entities because, where the Mitigation Plan related to multiple entities, Reliability*First* utilized the date of the last completion of mitigation activities as the date of Mitigation Plan completion. As noted above, however, the completion of mitigating activities within the Mitigation Plan may have varied from entity to entity. For additional information on the completion of mitigating activities and Mitigation Plans, please see section on Status of Mitigation Plans, below.

change management controls, configuration management controls, physical access controls, firewall controls, and a six-wall boundary.

Additionally, the UREs have implemented a private network for their Critical Asset substations, which isolates Critical Asset substation data traffic from all other bulk electric and distribution traffic and is isolated from the UREs' network by firewalls. Furthermore, the UREs control remote access to all Critical Asset substations through Parent Company's access control system, which utilizes two-factor authentication. Finally, the UREs control access privileges to ensure that only those individuals who meet the requirements of the CIP Reliability Standards are allowed authorized access to CCAs.

URE1's Violation of CIP-005-1 R3 (RFC201100969)

CIP-005-1 R3
CIP-005-1 R3 provides, in pertinent part:

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

CIP-005-1 R3.2 has a "Medium" VRF and a "Severe" VSL.

URE1 submitted a Self-Report to Reliability*First*, identifying a violation of CIP-005-1 R3. Within the Self-Report, URE1 stated its failure to ensure that its security monitoring processes alert designated response personnel, as specified by CIP-005-1 R3.2. URE1 also identified its IT personnel's failure to implement its processes for monitoring and responding to alerts, as specified by CIP-005-1 R3.2.

The UREs provided additional information to Reliability*First*, regarding URE1's noncompliance with CIP-005-1 R3. Specifically, the UREs stated that URE1 failed to review access logs for attempts at or actual

unauthorized accesses at least every ninety days where alerting was not technically feasible, as specified by CIP-005-1 R3.2.

URE1 violated CIP-005-1 R3 by failing to: (a) ensure that its security monitoring processes alert designated response personnel; (b) monitor and respond to alerts; and (c) review access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

Reliability*First* determined the duration of the violation was from when the Standard became mandatory and enforceable to when URE1 completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-005-1 R3 has the potential to affect the reliable operation of the BPS by providing the opportunity for individuals to access a Responsible Entity's ESP while leaving no record of the intrusion. Without having monitoring processes in place at access points, a Responsible Entity would be unable to detect and alert for unauthorized access to its ESP. Therefore, a Responsible Entity would be unable to prevent or track intrusions that could result in harm to the integrity of CCAs within the ESP. The risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. Although URE1's process for monitoring and logging access at access points to the ESP did not include issuing automated notifications when an alert was generated, URE1 represented that its staff members monitored the system twenty-four hours a day, seven days a week and received training regarding appropriate responses to any incidents. Furthermore, URE1 retained access logs beyond the 90 days required by CIP-005-1 R3, and upon its review of the access logs, URE1 did not identify any unauthorized attempts at or actual access to its EMS ESP. Therefore, URE1 had in place measures to detect and alert for unauthorized access to its ESPs and to protect Cyber Assets within the ESP, as well as access points to the ESP.

URE1's Violation of CIP-005-1 R4 (RFC201100970)

CIP-005-1 R4

CIP-005-1 R4 provides, in pertinent part:

> 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:
>
> * * * * *

R4.4. A review of controls for default accounts, passwords, and network management community strings;

* * * * *

CIP-005-1 R4 has a "Medium" VRF and a "Severe" VSL. URE1 submitted a Self-Report to Reliability*First*, identifying a violation of CIP-005-1 R4. Within the Self-Report, URE1 stated its failure to review controls for default accounts and network management community strings at the EMS and EBS ESP access points during the performance of its annual cyber vulnerability assessment, as specified by CIP-005-1 R4.4. Through the use of its previous system, URE1 was unable to update passwords on default accounts or network management community strings, and therefore, URE1 failed to include a requirement in its procedures that the cyber vulnerability assessment address default accounts and network community strings.

URE1 violated CIP-005-1 R4 by failing to review controls for default accounts and network management community strings during the performance of its annual cyber vulnerability assessment.

Reliability*First* determined the duration of the violation was from when the Standard became mandatory and enforceable to when URE1 completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-005-1 R4 has the potential to affect the reliable operation of the BPS by providing the opportunity for individuals to exploit vulnerabilities of a Responsible Entity's ESP access points of which the Responsible Entity is unaware. By exploiting vulnerabilities which would have been discoverable and preventable through the application of an annual cyber vulnerability assessment, an individual may gain unauthorized access to CCAs within the ESP and cause harm to the integrity of the CCAs.

The risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. Although URE1 did not review the default accounts and network management community strings during its cyber vulnerability assessments, URE1 located EMS and EBS CCAs and non-critical Cyber Assets within an established ESP and afforded these Cyber Assets with the protective measures required under CIP Reliability Standards CIP-005 and CIP-007. Therefore, the risk of unauthorized access to the EMS and EBS ESPs was reduced.

The UREs' Violations of CIP-005-1 R5 (RFC201100971 RFC2011001285, and RFC2011001286)

CIP-005-1 R5

CIP-005-1 R5 provides, in pertinent part:

> 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.

* * * * *

CIP-005-1 R5.1 has a "Lower" VRF and a "High" VSL. During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-005-1 R5 by concluding that URE1's documentation of the ESP for the EMS Network and EBS Network erroneously included a firewall that is not actually present in the ESP. URE1 therefore failed to maintain the documentation required by CIP-005 to reflect the current configurations and processes.

During the Compliance Audit of URE2 and URE3, Reliability*First* discovered URE2 and URE3's noncompliance with CIP-005-1 R1, which Reliability*First* determined also revealed noncompliance with CIP-005-1 R5. Specifically, URE2 and URE3 failed to ensure that their documentation of access points to their ESPs reflects the current configurations, when they failed to list four devices as access points to the ESP.

The UREs identified additional areas of URE2 and URE3's noncompliance with CIP-005-1 R1, which Reliability*First* determined also revealed noncompliance with CIP-005-1 R5. Specifically, URE2 and URE3 failed to reflect the current configuration of the infrastructure of URE2 and URE3's EMS network on the EMS ESP drawings, as specified in CIP-005-1 R5.

Additionally, all of the UREs provided additional information to Reliability*First*, regarding their noncompliance with CIP-005-1 R1, which also revealed noncompliance with CIP-005-1 R5. Specifically, upon completing their Cyber Vulnerability Assessments, the UREs discovered that several CCAs included on their substation CCA lists did not match the respective ESP drawings, as specified in CIP-005-1 R5.

The UREs violated CIP-005-1 R5 by failing to ensure all documentation required by Standard CIP-005 reflects current configurations and processes.

Reliability*First* determined the duration of URE2 and URE3's violations of CIP-005-1 R5 was from when the Standard became mandatory and enforceable to when URE2 and URE3 completed the Mitigation Plan. The duration of URE1's violation of CIP-005-1 R5 was from when the Standard became mandatory and enforceable to when URE1 completed the mitigating activities necessary to remedy the violation.[32]

Reliability*First* determined that these violations posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because the risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors. The UREs' violations related to incorrect ESP drawings. The UREs left no device unprotected as a result of this error. Additionally, the UREs established and implemented procedures to ensure that they control electronic access at all electronic access points to their ESPs. The UREs installed, implemented, and documented a multi-tiered access control system, which protected both their CCAs within their substations and the protection devices used to protect those locations, including certain devices. Furthermore, the UREs determined that even though their ESP diagrams for substations were not properly documented, the UREs accounted for these devices at these substations on the CCAs List, and afforded them the protections required under CIP-005-1 R1.

The risk posed by the violations was additionally reduced by the fact that the UREs had deployed firewalls and their access control system. The access control system securely communicates with Parent Company's Server, which authenticates those seeking access to the UREs' substations as well as its discrete devices, such as protective relays, RTUs, firewalls, and network switches. The UREs also had developed lists for the access control system and ensured that only personnel who have a functional need to access the devices are granted access.

The UREs' Violations of CIP-006-1 R1 (RFC201100972, RFC2011001287, and RFC2011001288)

CIP-006-1 R1

The purpose statement of 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. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

[32] The certification and verification documents provide that the Mitigation Plan was completed because that is the latest date of completion of mitigating activities within the Mitigation Plan.

CIP-006-1 R1[33] provides, in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
> >
> > 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).
> >
> > * * * * *
> >
> > R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.
> >
> > * * * * *
> >
> > 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.

[33] Versions 2 and 3 of CIP-006, R1 state, in pertinent part, "[t]he Responsible Entity shall document, ***implement***, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following…" (Emphasis added).
Additionally, the requirements listed within Version 1 of CIP-006, R1.8 are listed within CIP-006, R2.2 for Versions 2 and 3. For consistency within the Agreement, the Parties to the Agreement reference the originally applicable Standard and Requirement, CIP-006-1 R1.8, rather than the subsequently effective CIP-006-2 R2.2 or CIP-006-3 R2.2. Reliability*First* noted that Versions 2 and 3 of CIP-006 R2.2 differs from Version 1 of CIP-006 R1.8 by requiring a Responsible Entity to afford Cyber Assets used in the access control and monitoring of the PSP(s) with the protective measures specified in Standard CIP-006, Requirements R4 and R5. Since the facts and circumstances of the violations do not concern CIP-006, R4 and R5, this distinction between the version of CIP-006 had no bearing on the instant violations of CIP-006, R1.

CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; R1.7 and R1.8 each have a "Lower" VRF. ReliabilityFirst applied the VRF of CIP-006-1 R1 for a "Medium" VRF and a "Severe" VSL.

URE1 submitted a Self-Report to ReliabilityFirst, identifying a violation of CIP-006-1 R1.6. URE1 stated that it failed to implement its procedures for escorted access within the PSP for personnel not authorized with unescorted access, as specified by CIP-006-1 R1.6. Specifically, several log book entries were missing the time of the visitors' entries and exits, as well as the name of the escort for escorted visits.

URE1 submitted an additional Self-Report to ReliabilityFirst, identifying a violation of CIP-006-1 R1.8, and seven months later, the UREs provided additional information regarding the UREs' noncompliance with CIP-006-1 R1.8. The UREs stated that they did not comply with CIP-006-1 R1.8 when it failed to provide its devices used in the access control and monitoring of the PSPs with the protective measures specified in: CIP-003-1 R4 and R5; CIP-005-1 R2 and R3; CIP-007-1 R1 R2, R5, R6, and R9; CIP-009-1 R1, and R4.[34] Specifically, the UREs failed to: (a) include information related to 14 devices within its Information Protection Plan for identifying, classifying, protecting, and managing access to protected CCA information, as specified in CIP-003-1 R4 and R5; (b) document the configuration of ports and services required for operations for 14 devices, as specified in CIP-005-1 R2.2; (c) review the electronic access logs for 14 devices, as specified in CIP-005-1 R3; (d) ensure that significant changes to all 16 of its devices did not adversely affect existing cyber security controls, as specified in CIP-007-1 R1; (e) document the configuration of open ports and services to ensure that only those ports and services required for normal and emergency operations were enabled for 14 devices, as specified in CIP-007-1 R2; (f) implement its security patch management program on hardware patches and did not assess and apply one security patch on hardware, as specified in CIP-007-1 R3; (g) implement the technical and procedural controls that enforce access authentication of and accountability for all user activity, when it did not document a complete list of personnel with access to shared accounts for 14 devices, as specified in CIP-007-1 R5; (h) include 14 devices in the monitoring reports of system events that are related to cyber security, as specified in CIP-007-1 R6; (i) annually review and update the

[34] URE1 also provided information to ReliabilityFirst concerning URE1's failure to afford Cyber Assets used in the access control and monitoring of the PSP with the protective measures specified in CIP-007-1 R8; CIP-009-1 R2; and CIP-009-1 R5. ReliabilityFirst reviewed the information submitted by URE1 and determined that URE1 had resolved each of these areas of noncompliance, as documented within a previous settlement agreement. Therefore, ReliabilityFirst did not incorporate the facts related to URE1's noncompliance with CIP-007-1 R8; CIP-009-1 R2; and CIP-009-1 R5 within its violation of CIP-006-1 R1.

documentation listed in CIP-007-1 for 14 devices, as specified in CIP-007-1 R9; and (j) create and exercise recovery plans that apply to 14 devices, as specified in CIP-009-1 R1 and R4.[35]

Within the Self-Report and additional information, the UREs also stated that they did not comply with CIP-006-1 R1.8, when it failed to provide 30 control panel devices used in the access control and monitoring of the PSPs with the protective measures specified in: CIP-003-1 R4 and R5; CIP-005-1 R2 and R3; CIP-007-1 R1 R2, R3, R4, R5, R6, R8, and R9; CIP-008-1 R1; and CIP-009-1 R1 R2, R3, R4, and R5. Specifically, for these devices, the UREs failed to: (a) include information related to these devices within its Information Protection Plan for identifying, classifying, protecting, and managing access to protected CCA information, as specified in CIP-003-1 R4 and R5; (b) maintain documentation identifying which ports and services were required to be enabled for normal and emergency operations, including documentation of the configuration of ports and services required for operations for the devices, as specified in CIP-005-1 R2.2; (c) file a TFE where it was technically infeasible to display an appropriate use banner on the user screen of the devices upon all interactive access attempts, as specified in CIP-005-1 R2.6; (d) review the electronic access logs for these devices, as specified in CIP-005-1 R3.2; (e) create, implement, and maintain a cyber security test procedure for the devices, as specified in CIP-007-1 R1; (f) maintain documentation identifying the ports and services required to be enabled for normal and emergency operation, in order to ensure that only required ports and services were enabled for the devices, as specified in CIP-007-1 R2; (g) establish, document, and implement a security patch management process for the devices, as specified in CIP-007-1 R3; (h) use anti-virus software and other malicious software prevention tools to protect the devices or file a TFE where technically infeasible, as specified in CIP-007-1 R4; (i) implement the technical and procedural controls that enforce access authentication of and accountability for all user activity, when it failed to implement passwords meeting the complexity requirements, or file a TFE where technically infeasible, as specified in CIP-007-1 R5; (j) include the devices in the monitoring reports of system events that are related to cyber security, as specified in CIP-007-1 R6; (k) include the devices in the annual cyber vulnerability assessment of all Cyber Assets within the ESP, as specified in CIP-007-1 R8; (l) annually review and update the documentation required by CIP-007 for the devices, as specified in CIP-007-1 R9; (m) include the devices in their exercise of the Cyber Security Incident response plan, as specified in CIP-008-1 R1; (n) annually review, exercise, and update the Recovery Plan for the devices, as specified in CIP-009-1 R1 R2, and R3; (o) include processes and procedures for the backup and storage of the devices within its recovery plan, as specified in CIP-009-1 R4; and (p) test the backup media for the devices, as specified in CIP-009-1 R5.

Subsequently, during the URE1 Compliance Audit, Reliability*First* reviewed additional facts relating to URE1's compliance with CIP-006-1 R1 and concluded that URE1 failed to include all the information

[35] The R2 violation related to the annual exercise of the recovery plan was separately filed.

required by the sub-requirements of CIP-006-1 R1 within its physical security plan. Specifically, URE1 failed to ensure and document within its physical security plan that all Cyber Assets within an ESP also reside within an identified PSP, as specified in CIP-006-1 R1.1. Additionally, URE1 failed to identify all physical access points through each PSP, as specified in CIP-006-1 R1.2. URE1 also failed to document the processes, tools, and procedures to monitor physical access to the PSPs, as specified in CIP-006-1 R1.3. Finally, URE1 failed to establish and document a process to ensure that only those ports and services required for operations were enabled, and therefore failed to afford the protective measures specified in CIP-007 R2 to Cyber Assets used in the access control and monitoring of the PSPs, as specified in CIP-006-1 R1.8.

The UREs provided information to Reliability*First*, wherein they identified URE2 and URE3's noncompliance with CIP-006-1 R1. Specifically, the UREs stated that URE2 and URE3 share the same Physical Security Plan with URE1, and therefore, the URE1 Compliance Audit findings regarding URE1's failure to include all information required by the sub-requirements of CIP-006-1 R1 within its physical security plan also apply to URE2 and URE3. In particular, URE2 and URE3 failed to ensure and document within their physical security plan that all Cyber Assets within an ESP also reside within an identified PSP, as specified in CIP-006-1 R1.1. Additionally, URE2 and URE3 failed to identify all physical access points through each PSP, as specified in CIP-006-1 R1.2. URE2 and URE3 also failed to document the processes, tools, and procedures to monitor physical access to the PSPs, as specified in CIP-006-1 R1.3.

The UREs also described URE2 and URE3's failure to implement their procedures for escorted access within the PSP for personnel not authorized with unescorted access, as specified in CIP-006-1 R1.6. Specifically, URE2 and URE3 failed to maintain their log books with all information required by their procedures for escorted access within a PSP.

The UREs violated CIP-006-1 R1 by failing to address all the information required by the sub-requirements of CIP-006-1 R1 within their physical security plans.

Reliability*First* determined the duration of the violations was from when the Standard became mandatory and enforceable to when the UREs completed their Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-006-1 R1 has the potential to affect the reliable operation of the BPS by providing the opportunity to physically access Cyber Assets that are not protected by the implementation of a physical security plan. The risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by several factors.

The risk posed by the UREs' violations of CIP-006-1 R1.6 was mitigated by several factors. Although the UREs did not include some information on the visitor logs, the UREs represented that visitors were escorted at all times when within a PSP. Furthermore, the CCAs protected by the PSP have other security controls in place, including configuration management, change controls, patch management, malware protection, electronic and physical access controls, and system security monitoring.

The risk posed by the UREs' violations of CIP-006-1 R1.1 R1.2 and R1.3 was mitigated by the following factors. Although the UREs did not include all necessary information within their physical security plans, but rather they listed this information in separate documents and locations, the UREs did develop and maintain all required information. Furthermore, the UREs stored the PSP diagrams in a secure location with limited access, made them available to those with a need to know, and updated them when they introduced changes to the PSP. Finally, the PSP diagrams indicated the access points and other controls. A Security Operating Procedure outlined the tools and processes used to monitor and control access.

The risk posed by the UREs' failure to afford the protective measures listed in CIP-006-1 R1.8 to the control panel devices was mitigated by the fact that the UREs did provide the required CIP protections to the application itself. Specifically, the servers are protected from unauthorized electronic and physical access, monitored for system security, and subject to change controls, configuration management, malware prevention, patch management, and information protection. Additionally, in order to alter an individual's physical access rights to a PSP or affect access authorization or logging, a domain controller would need to authenticate the user, and the user would require authorization to access the application directly or through a workstation.

In addition to the protections provided directly to the application, the UREs had in place other security controls that protected the workstations and domain controllers from unauthorized physical and cyber access, as required under the UREs' standard IT security procedures. Specifically, although the UREs did not classify and label the information related to these devices as "NERC-Restricted," the workstations and domain controllers deny electronic access by default and required proper authorization. Additionally, the UREs controlled physical access to the workstations and domain controllers. Furthermore, the UREs provided malware protection to the domain controllers and the workstations. The control panels obtain all data on authorization privileges from the server, so the ability to impact the system negatively by accessing the control panels is very limited. Finally, all IT and Corporate Security personnel have PRAs and take annual NERC training to ensure that they are aware of the requirements of the CIP Reliability Standards.

The risk posed by the UREs' failure to afford the protective measures specified in CIP-003-1 R4 and R5 to Cyber Assets used in the access control and monitoring of the PSP was mitigated several facts. All of

the CCA information was corporate information that was already subject to standard security controls, under which the UREs denied electronic and physical access by default. Access was granted only to those who required it to perform their duties, and access was not granted until a designated approver submitted the required authorization. All personnel who had access to the CCA information had a PRA on file. Therefore, the information was protected from unauthorized physical and electronic access.

The risk posed by the UREs' failure to afford the protective measures specified in CIP-005-1 R2.2 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that the UREs had a process in place to limit ports and services. Specifically, although the UREs did not determine the initial baselines for ports and services that must be enabled for normal and emergency operations prior to the compliance date, the UREs used server build processes and standard operating procedures that were designed to limit open ports and services to those which are required according to vendor specification. The UREs deny access to Cyber Assets by default, so even if a port was not shut down, any unauthorized access attempts would be identified. Additionally, security controls are in place for these assets, including: configuration management, change controls, patch management, malware protection, electronic and physical access controls, and system security monitoring.

The risk posed by the UREs' failure to afford the protective measures specified in CIP-005-1 R2.6 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that the UREs display appropriate use banners on the login screen and the application. All authorized users of the server have completed NERC CIP training and are aware of the acceptable use policy, even where appropriate use banners are not displayed.

The risk posed by the UREs' failure to afford the protective measures specified in CIP-005-1 R3 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that the UREs' security monitoring process monitors the devices at issue. If an event had occurred that met the requirements established for potential incidents, the UREs would have issued an alert. The UREs have no recorded alerts for these devices during the time period of the violations.

The risk posed by the UREs' failure to afford the protective measures specified in CIP-007-1 R1 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that the access control panels are hardened single-purpose devices for which the cyber security testing consists only of port scans. These panels perform their access control and logging function by referencing a database of rules downloaded to the panel from a dedicated server. Account management and access level changes are not made at a panel level, but instead must be made through the server. The only changes made at the panel level are firmware upgrades. Furthermore, no panels have been significantly changed or replaced during the compliance period.

The risk posed by the UREs failure to afford the protective measures specified in CIP-007-1 R2 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that the UREs had other security controls in place, including configuration management, change controls, patch management, malware protection, electronic and physical access controls, and system security monitoring.

The risk posed by the UREs failure to afford the protective measures specified in CIP-007-1 R3 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the following factors. Although the UREs did not evaluate one patch within the 30-day period, the UREs did evaluate and apply all other patches released by the manufacturer of the two servers and seven domain controller servers. Furthermore, the server patches are cumulative, so the application of any patch release will update any that may not have been previously installed. Additionally, while the UREs did not apply functional patches to the Control panels, the UREs confirmed with the manufacturer of the panels that no security patches had been released for the access control panels during the time period of the violations.

The risk posed by the UREs' failure to afford the protective measures specified in CIP-007-1 R4 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that these control panels are hardened devices with proprietary operating systems that the vendor stated are not susceptible to common viruses and other malware.

The risk posed by the UREs' failures to afford the protective measures specified in CIP-007-1 R5 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that the UREs had procedural controls in place which required that all personnel utilize passwords meeting the password complexity requirements of CIP-007-1 R5.3. Furthermore, to access the application, a user must first login, wherein the UREs have implemented technical controls to enforce password length and annual password changes.

The risk posed by the UREs' failure to afford the protective measures specified in CIP-007-1 R6 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that they applied their existing procedures to these devices prior to reclassifying the devices. The UREs represented that those procedures address the system security monitoring requirements of CIP-007-1 R6.

The risk posed by the UREs' failure to afford the protective measures specified in CIP-007-1 R8 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that the UREs included some components of the System, namely the servers, domain controllers, and workstations, in the cyber vulnerability assessment. Additionally, the control panels are hardened single-purpose

devices with limited capabilities, no user accounts, and for which the cyber vulnerability assessment is limited to ports and services.

The risk posed by the UREs's failure to afford the protective measures specified in CIP-008-1 R1 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that the UREs demonstrated preparedness for incident response prior to reclassifying the devices. Specifically, they participated in a corporate exercise of the incident response plan and additionally utilized their then-current Corporate Security incident response procedure during an incident a year later (which was later determined not to be a cyber security incident).

The risk posed by the UREs' failures to afford the protective measures specified in CIP-007-1 R9 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that the technical documentation for the domain controllers was the same as that for the servers, which were not found to be out of compliance throughout the compliance period. Regarding the workstations, a special locked-down configuration was developed, and related procedures were documented prior to the devices being reclassified and brought into production. The UREs represented that there was no documentation to be reviewed prior to that time.

The risk posed by the UREs' failure to afford the protective measures specified in CIP-009-1 to Cyber Assets used in the access control and monitoring of the PSP was mitigated by the fact that while the UREs did not implement a formal recovery plan; the recovery process for the control panels involves replacing and reconfiguring failed devices, followed by the downloading of data from the server. The UREs carry out this process whenever the UREs install a control panel; therefore, the UREs had previously tested this process. Furthermore, the UREs store backup information on the server and on the backup server, both of which are monitored for successful completion. The UREs tested the restoration of the application and of the configuration backup to the server. The UREs conducted an additional test the following year, which included the control panels.

The UREs' Violations of CIP-007-1 R1 (RFC201100973, RFC2011001289, and RFC2011001290)

CIP-007-1 R1

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). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-007-1 R1 provides:

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

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

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

CIP-007-1 R1 has a "Medium" VRF and a "Severe" VSL.
URE1 submitted a Self-Report to Reliability*First*, identifying a violation of CIP-007-1 R1. URE1 failed to create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation, as required by CIP-007-1 R1.1. Specifically, URE1's Change Control Procedure failed to define "significant changes" or the cyber security controls that needed to be tested to ensure the cyber security controls were not adversely affected during a modification or change to Cyber Assets.

The UREs provided information to Reliability*First*, where they identified an additional area of URE1's noncompliance with CIP-007-1 R1. Specifically, during the course of implementing the Mitigation Plan and reviewing the evidence of completion, the UREs determined that the URE1 failed to maintain documentation showing that security patches were adequately tested before being installed on the production systems, as specified in CIP-007-1 R1.2 and R1.3.

The UREs provided information to Reliability*First*, wherein they identified URE2 and URE3's noncompliance with CIP-007-1 R1. Specifically, URE2 and URE3 failed to implement their cyber security test procedures in a manner that minimizes adverse effects on cyber security controls associated with the Cyber Assets, as required by CIP-007-1 R1.1. Additionally, URE2 and URE3 failed to perform testing of new Cyber Assets and significant changes to existing Cyber Assets within the ESP in a manner that reflects the production environment, as required by CIP-007-1 R1.2. Finally, because

URE2 and URE3 failed to perform the testing as required by CIP-007-1 R1.2, they additionally failed to document test results, as required by CIP-007-1 R1.3.

The UREs violated CIP-007-1 R1 by failing to create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation. Reliability*First* additionally determined that URE2 and URE3 violated CIP-007-1 R1 by failing to document that testing is performed in a manner that reflects the production environment and by failing to document test results.

Reliability*First* determined the duration of URE2 and URE3's violations of CIP-007-1 R1 was from when the Standard became mandatory and enforceable through when URE2 and URE3 completed the Mitigation Plan. Reliability*First* determined the duration of URE1's violation of CIP-007-1 R1 was from when the Standard became mandatory and enforceable to when URE1 completed the mitigating activities necessary to remedy the violation.[36]

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-007-1 R1 has the potential to affect the reliable operation of the BPS by providing the opportunity for new Cyber Assets within the ESP and significant changes to existing Cyber Assets within the ESP to adversely affect existing cyber security controls. The risk to the BPS was mitigated by several factors. The UREs had measures in place to secure their CCAs and non-critical Cyber Assets within the ESP. The UREs afforded their Cyber Assets with protective measures, including isolating Critical Asset substation data traffic from all other bulk electric and distribution traffic through the use of Parent Company's private network. This private network is also isolated from Parent Company's network by firewalls. Furthermore, the UREs control remote access to all Critical Asset substations through Parent Company's access control system, which utilizes two-factor authentication. In addition, the UREs control access privileges to ensure that only those individuals who meet the requirements of the CIP Reliability Standards are allowed authorized access to CCAs. Finally, the UREs represented that no incident or security breach occurred from the date of non-compliance to the present.

URE2 and URE3 afforded their Cyber Assets within the EMS ESP with protective measures to minimize unauthorized access, including firewall controls, access controls, user account controls, change management controls, physical access controls, and a six-wall boundary. Additionally, URE2 and URE3's EMS has a number of protective measures to minimize unauthorized access and ensure that access to the ESP and the Cyber Assets located within the ESP are secured and monitored. These

[36] The certification and verification documents state that the Mitigation Plan was completed on the date in which the last of the mitigating activities in the Mitigation Plan were completed.

protective measures include: firewalls on the ESP boundary, access controls, user account controls, change management controls, physical access controls, and a six-wall physical boundary.

Additionally, URE1 afforded its Cyber Assets with protective measures, including physical and cyber access controls, monitoring, anti-virus protection, and use of firewalls, which challenge any access attempts at all access points.

The UREs' Violations of CIP-007-1 R2 (RFC201000561, RFC201000582, and RFC201000540)

CIP-007-1 R2
CIP-007-1 R2 provides in pertinent part:

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

CIP-007-1 R2 has a "Medium" VRF and a "Severe" " VSL.
The UREs submitted a Self-Report to Reliability*First*, identifying a violation of CIP-007-1 R2. The UREs failed to maintain sufficient documentation to establish compliance with CIP-007-1 R2.1 and R2.2. Specifically, the UREs disclosed their failure to maintain documentation establishing that they had enabled only those ports and services required for normal and emergency operations and had disabled other ports and services.

Subsequently, the UREs informed Reliability*First* that they no longer believed that these facts constitute a violation. In support of this contention, the UREs submitted to Reliability*First* internal emails detailing work performed; however, Reliability*First* determined that these internal emails did not show that only those ports and services required for normal and emergency operations were enabled. Therefore, Reliability*First* determined that the UREs violated CIP-007-1 R2 by failing to enable only those ports and services required for normal and emergency operations and by failing to disable other ports and services.

During the URE1 Compliance Audit, Reliability*First* reviewed additional facts relating to URE1's compliance with CIP-007-1 R2, and concluded that URE1 failed to ensure that only those ports and services required for normal and emergency operations are enabled, as specified in CIP-007-1 R2. Specifically, URE1 failed to document the operational purpose of ports and services and failed to provide evidence to confirm that such ports and services are required for normal or emergency operations. The URE1 also failed to establish a baseline for the ports and services, and to compare changes made to the system to ensure that no new ports and services are open without URE1's knowledge, thereby creating the opportunity for new attack vectors.

Reliability*First* determined that the UREs violated CIP-007-1 R2 for failing to enable only those ports and services required for normal and emergency operations and failing to disable other ports and services.

Reliability*First* determined the duration of the violations was from when the Standard became mandatory and enforceable through when the UREs completed the mitigating activities necessary to remedy the violations.

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-007-1 R2 has the potential to affect the reliable operation of the BPS by providing the opportunity for infiltration of unauthorized network traffic into the ESP through ports and services that are not necessary for normal or emergency operations, but nevertheless remain enabled. The risk to the BPS was mitigated by several factors. The UREs implemented measures to detect and alert for infiltration of their Electronic Security Perimeters through ports and services. The UREs follow a defense-in-depth strategy to protect their CCAs. As part of this strategy, a third-party security service provider monitors sensors for traffic that traverses between corporate and substation networks. The managed security service provider did not identify any malicious traffic at any time.

The UREs' Violations of CIP-007-1 R2 (RFC2012009913, RFC2012009914, and RFC2012009915)

CIP-007-1 R2

CIP-007-1 R2.3 provides: "In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk."

CIP-007-1 R2.3 has a "Medium" VRF and a "Severe" VSL.

The UREs self-reported a violation of CIP-007-1 R2 to Reliability*First*. The UREs failed to document compensating measures applied to mitigate risk exposure or an acceptance of risk in instances where

unused ports and services cannot be disabled due to technical limitations, as required by CIP-007-1 R2.3. Specifically, during their completion of their cyber vulnerability assessment, the UREs determined that it was not technically feasible to disable unused ports and services for certain RTUs of all three of the UREs, three URE2 switches, and devices at URE2 and URE3. The UREs failed to document the compensating measures applied to mitigate risk exposure or an acceptance of the risk for each of these devices.

Reliability*First* determined that the UREs violated CIP-007-1 R2 by failing to document compensating measures applied to mitigate risk exposure or an acceptance of risk in instances where unused ports and services cannot be disabled due to technical limitations.

Reliability*First* determined the duration of the violations was from when the Standard became mandatory and enforceable through when the UREs completed their Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-007-1 R2 has the potential to affect the reliable operation of the BPS by providing the opportunity for infiltration of unauthorized network traffic into the ESP through ports and services that are not necessary for normal or emergency operations, but nevertheless remain enabled. The risk to the BPS was mitigated by several factors. The UREs follow a defense-in-depth strategy to protect their CCAs. As part of this strategy, a third-party security service provider monitored IDS sensors for traffic that traverses between corporate and substation networks. The managed security service provider did not identify any malicious traffic at any time. Therefore, the UREs had in place, at the time of the violations, measures to detect and alert for infiltration of their ESPs through ports and services.

The UREs' Violations of CIP-007-1 R3 (RFC201100974, RFC2011001291, and RFC2011001292)

CIP-007-1 R3
CIP-007-1 R3[37] 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

[37] Versions 2 and 3 of CIP-007 R3 state, in pertinent part, "[t]he 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…" (Emphasis added).

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.

URE1 submitted a Self-Report to Reliability*First*, identifying a violation of CIP-007-1 R3. URE1 stated that it failed to complete the assessment of one security patch within 30 calendar days of the availability of the security patch, as required by CIP-007-1 R3.1.

Subsequently, during the URE1 Compliance Audit, Reliability*First* reviewed additional facts related to URE1's compliance with CIP-007-1 R3, and concluded that the URE1 failed to install and document the implementation of certain security patches, and in any case where the patch was not installed, URE1 failed to document compensating measures applied to mitigate risk exposure, as required by CIP-007-1 R3.2.

The UREs submitted information to Reliability*First*, identifying noncompliance with CIP-007-1 R3. Specifically, the UREs stated that their security patch management program did not apply to all Cyber Assets within the ESP, particularly their field maintenance laptops. Therefore, the UREs failed to establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for their field maintenance laptops, as required by CIP-007-1 R3.

The UREs provided information regarding URE2 and URE3's noncompliance with CIP-007-1 R3 to Reliability*First*. Specifically, the UREs stated that URE2 and URE3 did not apply security patches to three operating systems and their applications, and therefore did not document an assessment or implementation of security patches for these three operating systems, as required by CIP-007-1 R3.1 and R3.2.

The UREs provided additional information to Reliability*First*, wherein they identified an additional area of URE1's noncompliance with CIP-007-1 R3. Specifically, during the course of implementing the Mitigation Plan and reviewing evidence of completion, the URE1 failed to install and document the assessment of 40 patches associated with its Update Server during the schedule specified by its patch management procedure for an entire year.

Reliability*First* determined that the UREs violated CIP-007-1 R3 by failing to: (a) document an assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades; (b) document the implementation of security patches; and (c) document compensating measures applied to mitigate risk exposure in any case where the patch was not installed. In addition, Reliability*First* determined that URE1 violated CIP-007-1 R3 by failing to establish and document a security patch management program for tracking, evaluating, testing, and installing applicable security software patches for its field maintenance laptops.

Reliability*First* determined the duration of URE2 and URE3's violations of CIP-007-1 R3 was from when the Standard became mandatory and enforceable to when URE2 and URE3 completed the mitigating activities necessary to remedy the violation. Reliability*First* determined the duration of URE1's violation of CIP-007-1 R3 was from when the Standard became mandatory and enforceable to when URE1 completed the Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-007-1 R3 has the potential to affect the reliable operation of the BPS by providing 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. The risk to the BPS was mitigated by several factors. The UREs had in place, at the time of the violations, controls to protect their systems from cyber security breaches. Specifically, the UREs have a private network for their Critical Asset substations which isolates Critical Asset substation data traffic from all other bulk electric and distribution traffic and is isolated from the UREs' Corporate IT network by firewalls. Furthermore, the UREs control remote access to all Critical Asset Substations through Parent Company's Corporate IT access control system, which utilizes two-factor authentication. Additionally, the UREs control access privileges to ensure that only those individuals who meet the requirements of the CIP Reliability Standards are allowed authorized access to CCAs.

In addition to the overall protections that the UREs provide to the CCAs located within their Critical Asset substations and ESPs, the UREs established and implemented a security patch management program which they followed for all devices other than the field maintenance laptops. The UREs follow these established patch and test procedures to evaluate, test, and apply security patches. Through their application of this patch management program, the UREs test security patches at a non-critical

substation before they are deployed to production systems. Concerning the field maintenance laptops, the UREs only utilize these field maintenance laptops locally to configure the protection relays, and the field maintenance laptops are not configured for remote access or with IP addresses. Additionally, the UREs represented that no incident or security breach occurred from the date of non-compliance to present.

Finally, the security patch relating to URE1's violation of CIP-007-1 R3, the patch, addressed a vulnerability that is exploitable only when using web servers connected to the Internet. The risk was reduced because URE1's Cyber Assets within the EMS and EBS ESPs do not have Internet access.

URE1's Violation of CIP-007-1 R3 (RFC201100975)

CIP-007-1 R3
CIP-007-1 R3.2 has a "Lower" VRF and "Severe" VRF.
During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-007-1 R3 by determining that URE1 failed to implement security patches, where technically feasible. URE1 also failed to implement the compensating and mitigating measures stated in URE1's TFE which URE1 filed with Reliability*First*.

Specifically, URE1's TFE Part B Summary states, "Parent Company's TNE [Telecommunications Network Engineering Group] has a plan in place to evaluate, document, and release/install applicable update security patches and Symantec AV signatures and patches for Critical Cyber Assets (servers, workstations). TNE has documented the evaluation of patches as applicable." During the URE1 Compliance Audit, URE1 failed to provide evidence indicating which patches were applied to each system and, therefore, failed to establish that URE1 followed its plan to "evaluate, document, and release/install" patches on applicable substation systems.

URE1 violated CIP-007-1 R3 by failing to implement security patches or the compensating and mitigating measures stated in its TFE.

Reliability*First* determined the duration of the violation was from when the Standard became mandatory and enforceable through when URE1 completed the mitigating activities necessary to remedy the violation.

Reliability*First* determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-007-1 R3 has the potential to affect the reliable operation of the BPS by providing 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. The risk to the BPS, during the pendency of the violation, was mitigated by several factors. The UREs had in place, at the time of the violations, measures to secure their CCAs in the absence of security patches. The UREs had in place, at the time of the violations, controls to protect their systems from cyber security breaches. Specifically, the UREs have a private network for their Critical Asset substationsthat isolates Critical Asset substation data traffic from all other bulk electric and distribution traffic and is isolated from the UREs' network by firewalls. Furthermore, the UREs control remote access to all Critical Asset substations through Parent Company's access control system, which utilizes two-factor authentication. Additionally, the UREs control access privileges to ensure that only those individuals who meet the requirements of the CIP Reliability Standards are allowed authorized access to Critical Cyber Assets. Thus, the UREs had in place, at the time of the violations, measures to secure their Critical Cyber Assets in the absence of security patches.

The UREs' Violations of CIP-007-1 R4 (RFC201100976, RFC2011001293, and RFC2011001294)

CIP-007-1 R4
CIP-007-1 R4 provides:

> R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
>
> > R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.
> >
> > R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

CIP-007-1 R4 has a "Medium" VRF and a "Lower" VSL.
URE1 self-reported to Reliability*First* a possible violation of CIP-007-1 R4. URE1 failed to test any of its anti-virus and malware prevention signatures prior to installing the signatures on its EMS production environment, as required by CIP-007-1 R4.2.

Subsequently, during the URE1 Compliance Audit, Reliability*First* reviewed additional facts related to URE1's compliance with CIP-007-1 R4, and concluded that URE1 failed to implement anti-virus software and other malicious software prevention tools on two CCAs, as specified in CIP-007-1 R4.1, and also failed to request a TFE for these two CCAs.

The UREs provided information to Reliability*First*, wherein they identified additional areas of the UREs' noncompliance with CIP-007-1 R4. Specifically, the UREs stated that they failed to test their anti-virus and malware prevention signatures to ensure that there is no adverse effect on the existing cyber security controls prior to installing the signatures, as specified in CIP-007-1 R4.2. Additionally, the URE2 and URE3 failed to install malware prevention tools or related signature files on their two backup servers, as specified in CIP-007-1 R4.1.

The UREs provided information to Reliability*First*, wherein they identified an additional area of URE1's noncompliance with CIP-007-1 R4. Specifically, during the course of implementing the Mitigation Plan and reviewing evidence of completion, the URE1 identified instances where it failed to test anti-virus signatures prior to applying the signatures in production systems for four months when URE1 experienced a technical issue with the installation of a version upgrade to a software program.

The UREs violated CIP-007-1 R4 by failing to implement a process for the update of anti-virus and malware prevention signatures and by failing to implement anti-virus and malware prevention tools.

Reliability*First* determined the duration of that URE2 and URE3's violations of CIP-007-1 R4 was from when the Standard became mandatory and enforceable through when URE2 and URE3 completed the mitigating activities necessary to remedy the violations. Reliability*First* determined the duration of URE1's violation of CIP-007-1 R4 was from when the Standard became mandatory and enforceable to when URE1 completed the mitigating activities necessary to remedy the violation.

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-007-1 R4 has the potential to affect the reliable operation of the BPS by providing the opportunity for the introduction, exposure, and propagation of malware on Cyber Assets within the ESP. The UREs implemented measures to provide protection against the threats of malware to their CCAs and non-critical Cyber Assets within their ESPs. The risk to the reliability of the BPS during the pendency of the violation posed by the foregoing facts and circumstances was mitigated by the following factors. The UREs provided technical controls to protect their systems from cyber security breaches. Specifically, the UREs have a private network for their Critical Asset substationswhich isolates Critical Asset substation data traffic from all other bulk electric and distribution traffic and is isolated from the UREs' network by firewalls. Furthermore, the UREs control remote access to all Critical Asset substations through Parent Company's Corporate IT

access control system, which utilizes two-factor authentication. Additionally, the UREs control access privileges to ensure that only those individuals who meet the requirements of the CIP Reliability Standards are allowed authorized access to CCAs. Finally, the UREs have determined that no incident or security breach occurred from the compliance date to the present.

In addition to the overall protections provided to the CCAs located within their Critical Asset substations ESPs, the UREs have an established malware prevention program in place, which they previously followed for all but two of their CCAs. The two CCAs cannot support malware prevention tools. The UREs have filed TFEs with Reliability*First* to document this technical infeasibility. The UREs currently follow their malware prevention program for all devices.

URE2 and URE3's violations related to two devices that disconnected to the Internet, located behind firewalls, only used four or five times per year for restoration operations, and are kept offline and powered down when not in use. For these reasons, the risk that these devices will fail, become infected with malware, or suffer a negative incident, is reduced. Additionally, these two devices are redundant, and only one is required to recover a system device. Therefore, in order for a failure to become an issue, three failures would be required: a system device failure plus failure of both of the devices.

URE1 affords its Cyber Assets within the EMS and EBS ESPs with protective measures, such as logging and monitoring, to mitigate the risk of unauthorized access or changes. In addition, although URE1 failed to test signatures within the test environment, URE1 installed these signatures into the production system, and the signatures performed as expected.

The UREs' Violations of CIP-007-1 R5 (RFC201100977, RFC2011001180, and RFC2011001181)

CIP-007-1 R5
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.
>
> > R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

* * * * *

R5.1.2.The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

* * * * *

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.

* * * * *

R5.2.3.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:

* * * * *

R5.3.2.Each password shall consist of a combination of alpha, numeric, and “special” characters.

* * * * *

CIP-007-1 R5 has a VRF of “Lower” VRF and “Severe” VSL.

URE1 submitted a Self-Report to Reliability*First*, identifying a violation of CIP-007-1 R5. URE1 had failed to implement its procedural controls regarding the frequency for changing passwords. Specifically, URE1's CIP-007 Account Management procedures require passwords to follow URE1's internal IT Security Standards, which require passwords to be changed every 90 days. URE1's EMS password policy did not implement this 90-day requirement, but instead required passwords to be updated annually.

Subsequently, during the URE1 Compliance Audit, Reliability*First* reviewed additional facts related to URE1's compliance with CIP-007-1 R5 and concluded that URE1 failed to generate logs of sufficient detail to create a historic audit trail of individual user account access activity for a minimum of 90 days, as required by CIP-007-1 R5.1.2. Specifically, URE1's log management system was out of service for 50 days in early 2011. As a result, URE1 failed to maintain logs during this time.

Additionally, during the URE1 Compliance Audit, Reliability*First* concluded that URE1 failed to require all CCAs to use passwords consisting of a combination of alpha, numeric, and "special" characters, as required by CIP-007-1 R5.3.2. Specifically, URE1 failed to establish, implement, and document technical controls that require an asset, located at a URE1 substation, to utilize a password consisting of a combination of alpha, numeric and special characters. Instead, the password for the asset consisted of a simple seven-digit number.

During the Compliance Audit of URE2 and URE3, Reliability*First* discovered URE2 and URE3's violations of CIP-007-1 R5. URE2 and URE3 had failed to require all CCAs use passwords consisting of a combination of alpha, numeric, and "special" characters, as required by CIP-007-1 R5.3.2. Specifically, URE2 and URE3 failed to establish, implement, and document technical controls that require devices to use passwords consisting of a combination of alpha, numeric, and "special" characters. URE2 and URE3 also failed to file a TFE where such technical controls were not technically feasible.

The UREs provided information to Reliability*First*, wherein they disclosed additional instances of URE2 and URE3's noncompliance with CIP-007-1 R5. Specifically, URE2 and URE3 failed to change passwords on required default accounts prior to putting their legacy EMS and system into service, as required by CIP-007-1 R5.2.1. URE2 and URE3 also failed to file a TFE where such password changes were not technically feasible. Finally, the URE2 and URE3 failed to maintain an audit trail of account use for their shared account on the EMS console, as required by CIP-007-1 R5.2.3**.**

The UREs violated CIP-007-1 R5 by failing to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity and that minimize the risk of unauthorized system access.

Reliability*First* determined the duration of that URE2 and URE3's violations of CIP-007-1 R5 was from when the Standard became mandatory and enforceable through when URE2 and URE3 completed the mitigating activities necessary to remedy the violations. The duration of URE1's violation of CIP-007-1 R5 was from when the Standard became mandatory and enforceable through when URE1 completed the mitigating activities necessary to remedy the violation.

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-007-1 R5 has the potential to affect the reliable operation of the bulk power system by providing the opportunity for unauthorized system access. The risk to the BPS was mitigated by several factors. The UREs implemented measures to protect against unauthorized system access to their CCAs and non-critical Cyber Assets within their ESPs. The UREs provide technical controls to protect their systems from cyber security breaches. The UREs have implemented a private network for their Critical Asset substations that isolates Critical Asset substation data traffic from all other bulk electric and distribution traffic. This private network is also isolated from the UREs' network through the use of firewalls. Additionally, although the UREs do not have technical controls, they have implemented procedural controls, which require that all personnel utilize passwords meet the requirements of CIP-007 R5.3.

Furthermore, the UREs control remote access to all Critical Asset substations through Parent Company's Substation access control system, which utilizes two-factor authentication. Therefore, in order to access the system, a person must first authenticate onto Parent Company's network, which utilizes complex passwords, then log onto the access control system, which requires two-factor authentication. Only after this process are the local shared passwords then utilized. For URE1, those shared passwords are further restricted on a "need to know" basis. Additionally, the UREs control access privileges to ensure that only those individuals who meet the requirements of the CIP Reliability Standards are allowed authorized access to CCAs.

URE1's CCAs within the EMS and EBS ESPs had other safeguards in place, including access controls, security patch management, change management procedures, anti-virus software, and firewall access controls. Additionally, URE1's automated tool is operational and monitoring the EMS.

URE2 and URE3 implemented additional protective features to ensure the security of the Cyber Assets within the EMS ESPs. In relation to the shared account, URE2 and URE3's EMS operators are only able to access the shared account after physically accessing the EMS control room, which is limited to those persons meeting the requirements of the CIP Reliability Standards for access to CCAs. The control room is staffed twenty-four hours a day, which provides an additional protection from staff members who would recognize an individual without authorized unescorted physical access logging onto the EMS console. Finally, the shared account only permits personnel to access limited data.

URE1's Violation of CIP-007-1 R5 (RFC201100978)

CIP-007-1 R5
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.
>
> * * * * *
>
> R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:
>
> * * * * *
>
> 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 "Lower" VRF and a "High" VSL.
During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-007-1 R5. URE1 failed to require the annual changing of passwords, where technically infeasible. URE1 did not follow the compensating and mitigating measures stated in three TFEs that URE1 filed with Reliability*First* and which Reliability*First* later approved. URE1 submitted evidence to Reliability*First* to demonstrate compliance with the terms of each TFE; however, in all three instances, Reliability*First* identified a violation of CIP-007-1 R5.

First, Section 6(i) of one TFE Part B Summary states that URE1 will restrict relay access to the server, the UREs' substation access control system, so that password changes can be made utilizing centralized servers, through which access to the server is granted. URE1 attempted to demonstrate that the servers require annual password changes; however, none of the documentation that URE1 submitted demonstrates the annual changing of passwords. Therefore, URE1 failed to follow the compensating measures for the server, as stated within its TFE.

Second, rather than utilizing complex passwords, as required by CIP-007-1 R5.3.2, URE1 stated in Section 6(i) of another TFE Part B Summary that it used the firewall access point to the ESP to block all native relay ports, thereby preventing direct cyber access to the relays. Despite this statement, URE1 did not implement this compensating measure. Instead, URE1 permitted external access to the substation network through a firewall, relays included within the TFE can be configured for remote user access, and the rule set for the firewall allowed inbound and outbound traffic to and from all devices on the substation network.

Third, in Section 6(i) of a third TFE Part B Summary, URE1 stated that it will restrict relay access to the server so that password changes can be made utilizing centralized servers. Despite this statement, URE1 did not implement this compensating measure. Instead, URE1 permitted external access to the substation network through a firewall, relays included within the TFE can be configured for remote user access, and the rule set for the firewall allowed inbound and outbound traffic to and from all devices on the substation network. Therefore, URE1 failed to restrict relay access to the server so that password changes, as specified in CIP-007-1 R5.3.3, can be made through the centralized servers.

URE1 violated CIP-007-1 R5 by failing to require and use passwords that are changed at least annually and, where such password changes were technically infeasible, by failing to follow the compensating and mitigating measures stated in three TFEs that URE1 filed with Reliability*First*.

Reliability*First* determined the duration of the violation was from when the Standard became mandatory and enforceable through when URE1 completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-007-1 R5 has the potential to affect the reliable operation of the BPS by providing the opportunity for unauthorized system access. The risk to the BPS was mitigated by several factors. URE1 provided technical controls to protect its systems from cyber security breaches. The UREs have implemented a private network for their Critical Asset substations that isolates Critical Asset substation data traffic from all other bulk electric and distribution traffic. This private network is also isolated from the UREs' Corporate IT network through the use of firewalls. Additionally, although the UREs did not have technical controls, they have implemented procedural controls, which require that all personnel utilize passwords that meet the requirements of CIP-007 R5.3.

Furthermore, the UREs control remote access to all Critical Asset substations through the UREs' Corporate IT access control system, which utilizes two-factor authentication. Therefore, in order to access the system, a person must first authenticate onto Parent Company's network, which utilizes complex passwords, then log on to the access control system, which uses two-factor authentication.

Only after this process are the local shared passwords then utilized. For URE1, those shared passwords are further restricted on a "need to know" basis. Additionally, the UREs control access privileges to ensure that only those individuals who meet the requirements of the CIP Reliability Standards are allowed authorized access to CCAs.

The UREs' Violations of CIP-007-1 R6 (RFC201100979, RFC2011001295, and RFC2011001296)

CIP-007-1 R6

CIP-007-1 R6 provides in pertinent part:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
>
> * * * * *
>
> R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
>
> R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
>
> R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

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

URE1 submitted a Self-Report to Reliability*First*, identifying a violation of CIP-007-1 R6. URE1 failed to document the organizational processes and technical and procedural mechanisms utilized by its security monitoring tool for monitoring for security events on all Cyber Assets within the ESP, as required by CIP-007-1 R6.

Subsequently, during the URE1 Compliance Audit, Reliability*First* reviewed additional facts related to URE1's compliance with CIP-007-1 R6 and concluded that the URE1 failed to ensure that all CCAs within the ESP automated tools or organizational process controls to monitor system events that are related to cyber security. Specifically, URE1 failed to maintain logs of system events related to cyber security to support incident response on two CCAs and failed to request a TFE for these two CCAs. Therefore, URE1 failed to implement its organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the ESP, as required by CIP-007-1 R6.1.

During the URE1 Compliance Audit, Reliability*First* also determined that URE1 failed to maintain logs of system events related to cyber security to support incident response. Specifically, URE1's log management system was out of service for 50 days. As a result, URE1 failed to maintain and review logs during this period, as required by CIP-007-1 R6.3, R6.4, and R6.5.

The UREs provided information to Reliability*First* regarding URE2 and URE3's noncompliance with CIP-007-1 R6. Specifically, the URE2 and URE3 failed to configure two CCAs, the Netbackup Boot Servers, to maintain logs of system events related to cyber security as required by CIP-007-1 R6.1. As a result, URE2 and URE3 did not maintain and review logs of system events, as required by CIP-007-1 R6.3, R6.4, and R6.5.

The UREs provided additional information to Reliability*First*, wherein they identified an additional area of noncompliance with CIP-007-1 R6. Specifically, the UREs did not document the processes and mechanisms for monitoring events on all Cyber Assets within the ESPs. Additionally, during the course of implementing their Mitigation Plan and reviewing evidence of completion, the UREs discovered that it was technically infeasible to monitor system events related to cyber security on three Ethernet switches at substations, as required by CIP-007-1 R6. The UREs also failed to file, with Reliability*First*, a TFE for the devices.

The UREs violated CIP-007-1 R6 by failing to ensure that all Cyber Assets within the ESPs implement automated tools or organizational process controls to monitor system events that are related to cyber security. URE1 violated CIP-007-1 R6 by failing to maintain logs of system events related to cyber security to support incident response.

Reliability*First* determined the duration of these violations was from when the Standard became mandatory and enforceable through the date the UREs completed their Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-007-1 R6 has the potential to affect the reliable operation of the BPS by providing the opportunity for undetected compromise of CCAs and

other system events that are related to cyber security to occur without the Responsible Entity's knowledge. The risk to the BPS was mitigated by several factors. The UREs had several measures in place to provide protection against system events to their CCAs and non-CCAs within their ESPs. The UREs implemented several compensating measures for the RTUs to ensure the security of the ESPs. The UREs' security controls are implemented in a layered architecture, which utilizes IDS, network firewalls, and two-factor authentication mechanisms. These mechanisms involve monitoring of the UREs' IDS event feeds, and the alerting of responsible personnel, twenty-four hours a day, seven days a week by an outside vendor in cases of potential cyber security-related incidents. Additionally, the UREs have installed IDS on both sides of the firewalls. Finally, users are only able to access the ESPs from the corporate IT network, which requires two-factor authentication.

The URE2's and URE3's violations relate to two devices that are not connected to the Internet, are located behind firewalls, are only used about four or five times per year for restoration operations, and are kept offline and powered down when not in use. Therefore the risk that these devices will fail, become infected with malware, or suffer a negative incident, is reduced. Furthermore, the URE2 and URE3 have implemented other protective measures to ensure the security of the Critical Cyber Assets within the EMS Electronic Security Perimeters. Specifically, URE2 and URE3 control remote access to all ESPs, and the Cyber Assets located within those ESPs, through the use of two-factor authentication to validate all users' access. The URE2 and URE3 also control and monitor access privileges to ensure that only those persons who meet the requirements listed within the CIP Reliability Standards are authorized to have access to CCAs.

URE1's CCAs within the EMS and EBS ESPs had other safeguards in place, including access controls, security patch management, change management procedures, anti-virus software, and firewall access controls. Further, URE1's automated tool is operational and monitoring the EMS. In addition, URE1 did not have any reportable Cyber Security Incidents since its start date of compliance and did not invoke CIP-008-3 Incident Reporting and Response Planning.

URE1's Violation of CIP-007-1 R8 (RFC201100981)

CIP-007-1 R8
CIP-007-1 R8 provides, in pertinent part:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> * * * * *

R8.3. A review of controls for default accounts;

* * * * *

CIP-007-1 R8 has a "Lower" VRF and a "Severe" VSL.
URE1 submitted a Self-Report to Reliability*First*, identifying a violation of CIP-007-1 R8. Although URE1 performed an annual cyber vulnerability assessment on all Cyber Assets within the ESP, this assessment failed to include a review of controls for default accounts, as required by CIP-007-1 R8.3.

URE1 violated CIP-007-1 R8 by failing to include a review of controls for default accounts within its annual cyber vulnerability assessment of all Cyber Assets within the ESP.

Reliability*First* determined the duration of the violation was from when the Standard became mandatory and enforceable through when URE1 completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-007-1 R8 has the potential to affect the reliable operation of the BPS by providing the opportunity for the system to be open to vulnerabilities that a Responsible Entity has failed to identify. The risk to the BPS was mitigated by several factors. URE1's EMS CCAs are located within an established ESP and are afforded protective measures, including firewalls which challenge any access attempts at all access points. Therefore, the risk of unauthorized personnel access within the ESP was reduced.

The UREs' Violations of CIP-008-1 R1 (RFC201100982, RFC2011001182, and RFC2011001183)

CIP-008-1 R1
The purpose statement of Reliability Standard CIP-008-1 provides in pertinent part: "Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-008-1 R1[38] provides, in pertinent part:

[38] Versions 2 and 3 of CIP-008 R1 state, in pertinent part, "[t]he Responsible Entity shall develop and maintain a Cyber Security Incident response plan ***and implement the plan in response to Cyber Security Incidents***." (Emphasis added).

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.

* * * * *

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

CIP-008-1 R1 has a "Lower" VRF and a "High" VSL.
During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-008-1 R1. URE1's Cyber Security Incident response plan did not: a) characterize and classify events as reportable Cyber Security Incidents, as required by CIP-008-1 R1.1; b) contain all response actions required by CIP-008-1 R1.2, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans; or c) contain a process for reporting incidents to the ES ISAC, as required by CIP-008-1 R1.3.

During the Compliance Audit of URE2 and URE3, Reliability*First* discovered violations of CIP-008-1 R1. URE2 and URE3 failed to test their Cyber Security Incident response plans annually. Specifically, although the URE2 and URE3 provided evidence demonstrating that their Cyber Security Incident response plans were reviewed at least annually, as required by CIP-008-1 R1.5, they were unable to provide evidence demonstrating that they tested the Cyber Security response plan annually, as required by CIP-008-1 R1.6.

URE1 violated CIP-008-1 R1 by failing to develop and maintain a Cyber Security Incident response plan that characterizes and classifies events as reportable Cyber Security Incidents, and that contains all

response actions required by CIP-008-1 R1.2, as well as a process for reporting incidents to the ES ISAC. Reliability*First* also determined that URE2 and URE3 violated CIP-008-1 R1 by failing to test their Cyber Security Incident response plans annually.

Reliability*First* determined the duration of URE2 and URE3's violations of CIP-008-1 R1 was from when the Standard became mandatory and enforceable through when URE2 and URE3 completed the mitigating activities necessary to remedy the violations. Reliability*First* determined the duration of URE1's violation of CIP-008-1 R1 was from when the Standard became mandatory and enforceable to when URE1 completed its Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-008-1 R1 has the potential to affect the reliable operation of the BPS by delaying a Responsible Entity's ability to respond, resolve, and recover from a Cyber Security Incident. The risk to the BPS was mitigated by several factors. The UREs had other mechanisms in place to protect CCAs against Cyber Security Incidents. No Cyber Security Incidents occurred during the time period of the noncompliance. Although URE2 and URE3 did not conduct an annual exercise of their Cyber Security Incident response plan, they did conduct an annual review of their Cyber Security Incident response plan. URE2 and URE3 afforded their Critical Cyber Assets with other protective measures to minimize threats and vulnerabilities, including: a) locating the Cyber Assets behind access points, including firewalls; b) implementing electronic and physical access controls to Critical Cyber Assets; c) implementing anti-virus software where technically feasible; and d) implementing user and system activity logging and monitoring.

The UREs' Violations of CIP-009-1 R1 (RFC201100983, RFC2011001184, and RFC2011001185)

CIP-009-1 R1

The Purpose Statement of Reliability Standard CIP-009-1 provides in pertinent part: "Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standard numbered Standards CIP-002 through CIP-009."

CIP-009-1 R1 provides:

> R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

CIP-009-1 R1 has a "Medium" VRF and a "Severe" VSL for URE1's violation and a "High" VSL for URE2 and URE3's violations.

URE1 submitted a Self-Report to Reliability*First*, identifying a violation of CIP-009-1 R1. URE1 had failed to create and annually review its recovery plan for CCAs, as required by CIP-009-1 R1. Specifically, for URE1's previous EMS system, URE1's recovery plan did not involve the recovery of individual CCAs that comprise the EMS, but instead required URE1 to switch to the EBS.

During the URE1 Compliance Audit, Reliability*First* reviewed additional facts related to URE1's compliance with CIP-009-1 R1 and concluded that the URE1 failed to create and exercise annually a recovery plan for CCAs.

During the URE1 Compliance Audit, Reliability*First* also concluded that URE1's recovery plan for substations did not specify the actions required in response to events or conditions of varying duration and severity which would activate the recovery plan, as required by CIP-009-1 R1.1. Reliability*First* further concluded that URE1 failed to define the roles and responsibilities of responders, as required by CIP-009-1 R1.2.

During the Compliance Audit of URE2 and URE3, Reliability*First* discovered violations of CIP-009-1 R1. Specifically, URE2 and URE3's recovery plan did not involve the recovery of individual CCAs that comprise the EMS, as required by CIP-009-1 R1. Additionally, URE2 and URE3's recovery plan did not specify the actions required in response to events or conditions of varying duration and severity which would activate the recovery plan, as required by CIP-009-1 R1.1.

The UREs violated CIP-009-1 R1 by failing to create and annually review their recovery plans for CCAs.

Reliability*First* determined the duration of URE2 and URE3's violations of CIP-009-1 R1 was from when the Standard became mandatory and enforceable through when URE2 and URE3 completed the mitigating activities necessary to remedy the violations. The duration of URE1's violation of CIP-009-1 R1 is from when the Standard became mandatory and enforceable to when URE1 completed the mitigating activities necessary to remedy the violation.

ReliabilityFirst determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-009-1 R1 has the potential to affect the reliable operation of the BPS by providing the opportunity for a delay in the Responsible Entity's recovery of a failed CCA. The risk to the BPS was mitigated by several factors. The UREs had mechanisms in place to protect CCAs against system events. URE1 backed up and stored the information required to restore CCAs in the form of tapes from the backup EMS and the disaster backup EMS. URE1 also maintained the vendor's instructions for recovering individual Cyber Assets, even though it had not incorporated these vendor instructions into its recovery plan. Historically, URE2 and URE3 have successfully restored various types of failed assets utilizing the vendor instructions. In addition, URE2 and URE3 afforded their Cyber Assets protective measures to reduce the risk of failure and minimize threats and vulnerabilities. Those protective measures included: a) locating the Cyber Assets behind access points, including firewalls; b) implementing electronic and physical access controls to all Cyber Assets within the ESP and ESP access points; c) implementing anti-virus software where technically feasible; and d) implementing user and system activity logging and monitoring of access points and Cyber Assets within the ESP.

URE1's Violation of CIP-009-1 R2 (RFC201100984)

CIP-009-1 R2

CIP-009-1 R2 provides: "Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident."

CIP-009-1 R2 has a "Lower" VRF and a "Severe" VSL.

URE1 submitted a Self-Report to ReliabilityFirst, identifying a violation of CIP-009-1 R2. URE1 failed to exercise its recovery plan annually, as required by CIP-009-1 R1. Due to URE1's failure to create a recovery plan, URE1 also failed to exercise a recovery plan annually as required by CIP-009-1 R2.

Subsequently, during the URE1 Compliance Audit, ReliabilityFirst reviewed additional facts related to URE1's compliance with CIP-009-1 R2. ReliabilityFirst confirmed the information identified within URE1's Self-Report and concluded that URE1 failed to exercise the recovery plan annually.

URE1 had a violation of CIP-009-1 R2 for failing to exercise its recovery plan annually.

ReliabilityFirst determined the duration of the violation was from when the Standard became mandatory and enforceable to when URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-009-1 R2 has the potential to affect the reliable operation of the BPS by providing the opportunity for a delay in the Responsible Entity's response to an actual incident or recovery of a failed CCA. The risk to the BPS was mitigated by several factors. Although URE1 did not annually exercise its recovery plan, it did conduct restoration exercises for the entire EMS after that date. Additionally, URE1 conducted a recovery plan exercise, including exercises of the EMS Backup System, to ensure that adequate backup or replacements would be available if needed.

URE1's Violation of CIP-009-1 R3 (RFC201100985)

CIP-009-1 R3.
CIP-009-1 R3 provides: **"**Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change."[39]

CIP-009-1 R3 has a "Lower" VRF and a "Severe" VSL.

URE1 submitted a Self-Report to ReliabilityFirst, identifying a violation of CIP-009-1 R3. URE1 failed to update its recovery plan to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident for its legacy EMS. URE1 had also failed to communicate changes to the appropriate personnel.

URE1 had a violation of CIP-009-1 R3 for failing to update its recovery plan to reflect changes or lessons learned as a result of an exercise or the recovery from an actual incident.

ReliabilityFirst determined the duration of the violation was from when the Standard became mandatory and enforceable through when URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-009-1 R3 has the potential to affect the reliable operation of the BPS by providing the opportunity for a delay in the Responsible Entity's

[39] Versions 2 and 3 of CIP-009, R3 state, in pertinent part, "…[u]pdates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) ***within thirty calendar days*** of the change being completed." (Emphasis added).

response to an actual incident, due to the Responsible Entity's lack of familiarity with previous incidents. The risk to the BPS was mitigated by several factors. Although URE1 did not maintain documentation demonstrating its communication of changes to appropriate personnel, URE1 did notify necessary personnel of the changes on an informal basis. Additionally, URE1 created a draft of its recovery plan procedures (Draft Version 0) and utilized this Draft Version 0 to test two devices on its new EMS system. URE1 updated Draft Version 0 based on the exercise (Draft Version 1), and URE1 utilized Draft Version 1 to test six additional devices on its new EMS system. URE1 then updated Draft Version 1 to reflect lessons learned from the exercise. All individuals of URE1's EMS Support Staff were involved in the implementation of the new EMS system, as well as in updating the draft versions of the recovery plan procedures. Therefore, while URE1 did not implement an approved recovery plan, it ensured that it updated its draft recovery plan to reflect changes and lessons learned and communicated those updates to relevant personnel, which ensured that URE1 familiarized its personnel with lessons learned to protect its CCAs against system events.

The UREs' Violations of CIP-009-1 R4 (RFC201100986, RFC2011001299, and RFC2011001300)

CIP-009-1 R4

CIP-009-1 R4 provides: "Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc."

CIP-009-1 R4 has a "Lower" VRF and a "Severe" VSL.
During the URE1 Compliance Audit, Reliability*First* discovered a violation of CIP-009-1 R4. URE1 had failed to include processes and procedures for the backup and storage of information required to successfully restore CCAs within its recovery plan.

Although URE1 had a standalone backup and restore procedure for the EMS, URE1 did not include this procedure within its recovery plan, because URE1 did not have a recovery plan. Additionally, URE1's substation backup and restore procedures did not contain processes and procedures for the backup and storage of information required to successfully restore CCAs.

The UREs provided information to Reliability*First* regarding URE2 and URE3's noncompliance with CIP-009-1 R4. Specifically, URE2 and URE3 did not include appropriate processes and procedures in their recovery plans for the backup and storage of information required to restore their two backup servers successfully. Instead, URE2 and URE3's procedures for the backup servers were circular in nature. The procedures required the use of the failed backup boot servers in order to restore those same servers.

Should any event occur, URE2 and URE3 would therefore be unable to restore the backup servers, as specified in CIP-009-1 R4.

The UREs had a violation of CIP-009-1 R4 for failing to include processes and procedures for the backup and storage of information required to successfully restore CCAs within their recovery plans.

Reliability*First* determined the duration of URE2 and URE3's violations of CIP-009-1 R4 was from when the Standard became mandatory and enforceable through when URE2 and URE3 will complete their Mitigation Plan. Reliability*First* determined the duration of URE1's violation of CIP-009-1 R4 was from when the Standard became mandatory and enforceable through when URE1 completed the mitigating activities necessary to remedy the violation.

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-009-1 R4 has the potential to affect the reliable operation of the BPS system by providing the opportunity for a delay in the Responsible Entity's restoration of CCAs. The UREs implemented controls to ensure the business continuity and security of their CCAs. The risk to the BPS was mitigated by several factors. URE1 exercised its standalone backup and restore procedure for the EMS. Additionally, the URE1 maintained paper copies of the configuration files for its CCAs, as well as backup information that would enable the successful restoration of its CCAs. URE1 also did not have any instances in which it was necessary to retrieve backup information for the restoration of its CCAs.

URE2 and URE3's violations relate to two devices that are not connected to the Internet. They are located behind firewalls, only used about four or five times per year for restoration operations, and kept offline and powered down when not in use. The risk that these devices will fail, become infected with malware, or suffer a negative incident, is reduced. Additionally, these devices are redundant, because only one is required to recover a system device. In order for a failure to become an issue, three failures would be required - a system device failure plus failure of both of the devices. The URE2's and URE3's support staffs were trained to recover these devices. Furthermore, URE2 and URE3 have vendor documentation that describes the steps involved in the restoration process for the boot servers, which also allowed appropriate personnel to gain familiarity with the restoration process.

URE2 and URE3 have a number of other protective measures to ensure the security of the EMS CCAs. Specifically, URE2 and URE3 control remote access to all ESPs and the Cyber Assets located within those ESPs, through the use of two-factor authentication to validate all users' access. Finally, URE2 and URE3 control and monitor access privileges to ensure that only those persons who meet the requirements listed within the CIP Reliability Standards are authorized to have access to CCAs.

The UREs' Violations of CIP-009-1 R5 (RFC201100987, RFC2011001186, and RFC2011001187)

CIP-009-1 R5

CIP-009-1 R5 provides: **"**Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site."

CIP-009-1 R5 has a "Lower" VRF and a "Severe" VSL.
URE1 submitted a Self-Report to Reliability*First*, identifying a violation of CIP-009-1 R5. URE1 failed to test annually the backup media to ensure that information essential to the recovery of CCAs that was stored on backup media for its legacy EMS was available.

During the Compliance Audit of URE2 and URE3, Reliability*First* discovered URE2 and URE3's noncompliance with CIP-009-1 R5. URE2 and URE3 had failed to test annually backup media to ensure that the information is available. URE2 and URE3 had backups of the networking devices configurations on other servers, but they did not conduct an annual test of this media in 2010.

The UREs had a violation of CIP-009-1 R5 for failing to test annually the information essential to recovery that is stored on backup media to ensure the information was available.

Reliability*First* determined the duration of URE2 and URE3's violations of CIP-009-1 R5 was from when the Standard became mandatory and enforceable through when URE2 and URE3 completed the mitigating activities necessary to remedy the violations. Reliability*First* determined the duration of URE1's violation of CIP-009-1 R5 was from when the Standard became mandatory and enforceable through when the Mitigation Plan was completed.

Reliability*First* determined that these violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS because a violation of CIP-009-1 R5 has the potential to affect the reliable operation of the BPS by providing the opportunity for the prevention of or a delay in the Responsible Entity's restoration of CCAs. The risk to the BPS was mitigated by several factors. URE2 and URE3 afforded their Cyber Assets other protective measures to reduce the risk of failure and minimize threats and vulnerabilities. Those protective measures included: a) locating the Cyber Assets behind access points, including firewalls; b) implementing electronic and physical access controls to all Cyber Assets within the ESP and ESP access points; c) implementing anti-virus software where technically feasible; and d) implementing user and system activity logging and monitoring of access points and Cyber Assets within the ESP. Furthermore, upon testing the network device backup media during their mitigating activities, URE2 and URE3 confirmed that information was available and the test was successful. Therefore, the UREs had implemented other mechanisms to maintain the information

essential to recovery. URE1 had backed up and stored the information required to successfully restore CCAs in the form of the tapes from the EMS and the disaster backup EMS.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, Reliability*First* has assessed a penalty of seven hundred twenty-five thousand dollars ($725,000) for the referenced violations. In reaching this determination, Reliability*First* considered the following factors:

1. Reliability*First* considered the UREs' lack of a culture of compliance regarding the CIP Reliability Standards at the time Reliability*First* discovered the violations at issue in this Agreement. Reliability*First* determined the UREs had a lack of familiarity with their CIP processes and procedures and a failure to implement those processes and procedures. Additionally, Reliability*First* noted that responsibility for compliance with CIP Reliability Standards at the UREs was spread among six separate executives, thereby reducing ownership of the compliance processes and causing inconsistent application of these processes;
2. Reliability*First* considered the UREs' subsequent strides toward fostering a culture of compliance following the discovery of the violations. Upon discovering the violations, the UREs immediately began working with Reliability*First* to remedy the violations and to create an improved compliance program going forward;
3. The UREs' collaboration with Reliability*First* was evidenced through the UREs' participation in numerous in-person meetings and conference calls with Reliability*First* personnel. For example, Reliability*First* executives engaged executives of the UREs to ensure the UREs' organizational commitment to address the violations. During a separate meeting, the UREs presented their compliance initiative to Reliability*First* personnel and requested Reliability*First*'s feedback regarding their progress in returning to compliance with the CIP Reliability Standards. Additionally, the UREs completed weekly conference calls with Reliability*First* personnel to discuss the ongoing progress of mitigating activities;[40]
4. Through these interactions, the UREs demonstrated a willingness to collaborate with Reliability*First* in order to maximize the reliability benefits associated with Reliability*First*'s CMEP activities. For these reasons, Reliability*First* considered the UREs' overall cooperation with Reliability*First* during the enforcement process to constitute a mitigating factor for penalty purposes;
5. The UREs also implemented a compliance initiative aimed at restructuring departments and personnel to enforce compliance with Reliability Standards, refocusing senior management

[40] The Settlement Agreement states that the UREs completed weekly conference calls with Reliability*First* personnel to discuss the ongoing progress of mitigating activities.

leadership toward compliance activities, standardizing compliance procedures, monitoring mitigation activities, and implementing controls to ensure future compliance. For the reasons discussed below, Reliability*First* considered the UREs' implementation of the compliance initiative to warrant mitigating credit for penalty purposes;

6. Within this compliance initiative, the UREs expanded their compliance staff and enhanced their compliance roles and responsibilities. The UREs created the position of Chief Compliance Officer (CCO), who is responsible for leading Parent Company's Corporate Compliance organization and corporate compliance efforts, including with respect to NERC compliance activities. The CCO works closely with senior management, including directly reporting to the Senior Vice President and General Counsel and having access to the Audit Committee of the Board of Directors. The CCO also works closely with subject matter experts in relevant departments to develop and advance a culture of compliance built upon the implementation of rigorous subject area compliance plans;
7. Additionally, the UREs identified Executive Standards Owners for each CIP Reliability Standard to maintain an active and visible role in supervising compliance, participating in a NERC Steering Committee, and overseeing the completion of compliance tasks by personnel across the UREs. Furthermore, the UREs filled the designated compliance positions of Standards Managers, who are responsible for ensuring that key tasks are assigned, tracked, and completed on a timely basis, and are critical to the UREs' ongoing compliance efforts;
8. Within the Parent Company Compliance Department, the UREs also added a position of Compliance Manager to handle Cyber Security and routinely meet with Standards Managers to plan for continuous improvement goals, self-certification strategy, annual internal reviews of tasks and spot checks, and annual risk analysis. Within the same department, the UREs also added a position of Principal Consultant to manage compliance enforcement correspondence between both Cyber Security and Operations & Planning NERC Compliance. The UREs have structured additional measures and timelines to hire additional full time employees identified by the compliance initiative;
9. In addition to the hiring of personnel and restructuring of roles and responsibilities, the UREs have included other activities within their compliance initiative to promote and foster their improved culture of compliance. The UREs are unifying their corporate procedures to ensure the standardization of procedures, processes, and other documents, which will ensure compliance across functional areas of each of the UREs;
10. The UREs are also in the process of changing their manual compliance forms into an automated online system of forms and workflows in an effort to standardize fields and forms; expedite workflows; and improve document accuracy and completeness, version control, and document storage and retrieval.

11. The UREs are in the process of building an intelligence network to connect key substations which will increase the UREs' physical security by facilitating physical access monitoring and surveillance, providing video enhancing physical security forensics, enhancing physical security at unmanned facilities, and increasing efficiencies in the badge process for remote sites;

12. Furthermore, the UREs are implementing a security event monitoring and automated alert tool to add additional security to their EMS ESP devices. This tool monitors and alerts for possible attacks or intrusions by monitoring real-time file and configuration changes on all EMS Electronic Security Perimeter devices;

13. The UREs are also implementing a document repository to ensure accurate document management, task tracking, and standardized retention of compliance evidence;[41]

14. Reliability*First* favorably considered the fact that the UREs self-reported many of the violations and therefore assigned mitigating credit for those violations which Reliability*First* had not discovered during the URE1 Compliance Audit or the Compliance Audit of URE2 and URE3. Reliability*First* did not assign mitigating credit to those violations which URE1 self-reported on the eve of the URE1 Compliance Audit and which were then investigated during the URE1 Compliance Audit;[42]

15. When assessing the penalty for the violations at issue in the Settlement Agreement, Reliability*First* considered whether the facts of these violations evidenced: a) repeated or continuing conduct similar to that underlying the prior violation of the same or a closely-related Reliability Standard Requirement; b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or c) multiple violations of the same Standard and Requirement; and

16. The UREs and Reliability*First* have also agreed to actions that the UREs will take to exceed baseline compliance. The UREs estimate this commitment will cost approximately $350,000, exclusive of any mitigation measures that may be required as a result of data collected. The commitment described within the Settlement Agreement enhances the reliability of the BPS beyond baseline compliance with the Reliability Standards, and therefore Reliability*First* viewed it in a favorable light in conjunction with the overall level of penalty and other terms and conditions of the Agreement. Reliability*First* will monitor the UREs' implementation of this

[41] The UREs have installed the document repository on the development system and are in the process of testing it. The repository is part of a larger compliance management effort, and the UREs plans to complete training on the new system for all compliance personnel prior to going live.

[42] RFC201100964, RFC201100965, RFC201100969, RFC201100970, RFC201100973, RFC201100981, RFC201100985, RFC201100987, RFC2011001276, RFC2011001277, RFC2012010075, RFC2012010076, RFC2011001283, RFC2011001284, RFC2011001289, RFC2011001290, RFC201000561, RFC201000582, RFC201000540, RFC2012009913, RFC2012009914, RFC2012009915, RFC2011001293, and RFC2011001294 received self-reporting credit.

commitment in accordance with the CMEP.[43]

After consideration of the above factors, Reliability*First* determined that, in this instance, the penalty amount of seven hundred twenty-five thousand dollars ($725,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[44]

URE1's Violation of CIP-002-1 R1 (RFC201100957)

URE1's Mitigation Plan to address its violation of CIP-002-1 R1 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE1 certified that the above Mitigation Plan requirements were completed. URE1 submitted evidence of completion of its Mitigation Plan.

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

URE1's Violation of CIP-002-1 R2 (RFC201100958)

URE1's Mitigation Plan to address its violation of CIP-002-1 R2 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE1's Mitigation Plan required URE1 to:

[43] The UREs commit to perform ongoing cyber security risk analysis, using a Failure Modes Effects Analysis ("FMEA") tool to review the UREs' cyber security policies and procedures, in order to minimize or eliminate CIP compliance failures. The UREs will utilize the FMEA to analyze the potential process failures and gaps in their CIP compliance processes and procedures, through the review of previous instances of compliance and noncompliance with the CIP Reliability Standards. This review will allow the UREs to design previous failures out of the system. Through the use of the FMEA, the UREs will perform periodic cyber security risk analysis to identify potential failures and to prioritize the remediation of such failures based on the potential severity and likelihood of occurrence.

[44] *See* 18 C.F.R § 39.7(d)(7).

1. Update the revision history for the CA lists to include a RBAM version reference column to ensure that the version of the RBAM on which each Critical Asset list version was based is readily apparent;

2. Review its Critical Asset list to ensure all control centers, BES substations and non-BES blackstart path substations are identified to be evaluated as Critical Assets;

3. Update the revision history for the Substation CCA lists to include a Critical Asset list version reference column to ensure that the version of the Critical Asset list on which each CCA list version was based is readily apparent.

URE1 certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE1 submitted the following:

1. Critical Assets list; this list was based on the Version 4 of the *Risk-Based Assessment Methodology*.

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

URE1's Violation of CIP-002-1 R3 (RFC201100959)

URE1's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to Reliability*First*. URE1 submitted an amended Mitigation Plan. Reliability*First* accepted the amended Mitigation Plan and NERC approved it. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE1's Revised Mitigation Plan required URE1 to modify its CCA list to reference the Critical Asset list used for identifying CCAs. Additionally, URE1 removed the criterion in its procedure for the identification of CCAs which required the identification of Cyber Assets affecting "the loss of at least [XXX] mw [sic] of load." Finally, URE1 detailed the steps it will take to ensure accurate labeling of CCAs, including training for employees regarding the proper designation for devices on the list of CCAs.

URE1 certified that the above Mitigation Plan requirements were completed. URE1 submitted evidence of completion of its Mitigation Plan.

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

URE1's Violation of CIP-002-1 R4 (RFC201100960)

URE1 submitted a Mitigation Plan to address its violation of CIP-002-1 R4 to Reliability*First*. URE1 submitted an amended Mitigation Plan to address the violation of CIP-002-1 R4 to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE1's revised Mitigation Plan required URE1 to:

1. Update its cyber security policy to clarify the wording of the Parent Company "annual" definition to specify meaning of once per calendar year and move the term "annual" from the end notes to the Glossary of Terms section;

2. Review and update its RBAM annually. URE1 had revised the RBAM approval signature page and it is part of the RBAM document. The Senior Manager had approved the RBAM;

3. Review and update its list of Critical Assets annually. URE1 had revised the approval signature page for its list of Critical Assets. The approval signature page is part of the list of Critical Assets document. The Senior Manager approved the list of Critical Assets;

4. Review and update its list of Substation CCAs annually. URE1 revised the approval signature page for its list of Substation CCAs to include reference to the version of RBAM. The Senior Manager approved the list of Substation Critical Assets;

5. Modify the Version Control and Tracking page in its Critical Asset list used for identifying CCAs. A review and signature table was to be added to clarify when the CIP Senior Manager approved the list; and

6. Ensure that its CIP-002 documentation identifies those Critical Asset Substations without CCAs.

URE1 certified that the above Mitigation Plan requirements were completed. URE1 submitted evidence of completion of its Mitigation Plan.

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

URE1's Violation of CIP-003-1 R1 (RFC201100961)

URE1's Mitigation Plan to address its violation of CIP-003-1 R1 was submitted to Reliability*First* with an expected completion date. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE1's Mitigation Plan required URE1 to:

1. Publish the "Cyber Security Policy for Parent Company PD Bulk Electric Systems" on the Parent Company intranet site to permit all employees with access to a corporate computer and appropriate log-in credentials to view the current document. For those individuals or contractors who did not have access to the corporate intranet site, Parent Company required they read a hard copy of the "Cyber Security Policy for Parent Company PD Bulk Electric Systems";
2. Hold formal annual review meetings with business unit stakeholders to ensure that individual departmental policies and plans conform to and address all requirements described in "Cyber Security Policy for Parent Company PD Bulk Electric Systems"; and
3. The Senior Manager at Parent Company will approve any changes to the "Cyber Security Policy for Parent Company PD Bulk Electric Systems" and confirm that it meets the requirements of CIP-003 R1 on an annual basis.

URE1 certified that the above Mitigation Plan requirements were completed. URE1 submitted evidence of completion of its Mitigation Plan.

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

URE1's Violation of CIP-003-1 R5 (RFC201100962)

URE1's Mitigation Plan to address its violation of CIP-003-1 R5 was submitted to Reliability*First*. URE1 submitted an amended Mitigation Plan to address the violation of CIP-003-1 R5 to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation and was submitted as non-public information to FERC in accordance with FERC orders.

URE1's Mitigation Plan required URE1 to document and implement procedures for managing access to protected CCA information and to establish an annual review for controlling access privileges to protected information. URE1 trained all necessary personnel on the new procedure. URE1 also

created and now maintains a list of designated personnel who are responsible for authorizing access to protected information. Finally, URE1 reviewed the access privileges to protected information to confirm that access privileges are correct and that they correspond with URE1's needs and appropriate personnel roles and responsibilities.

URE1 certified that the above Mitigation Plan requirements were completed. URE1 submitted evidence of completion of its Mitigation Plan.

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

The UREs' Violations of CIP-003-1 R6 (RFC201100963, RFC2011001274, and RFC2011001275)

The UREs' Mitigation Plan to address their violations of CIP-003-1 R6 was submitted to Reliability*First*. The UREs submitted an amended Mitigation Plan to address the violations of CIP-003-1 R6 to Reliability*First* with separate completion dates for URE1, URE2 and URE3. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs' to: (i) implement a configuration management tool on all CCAs within the EMS and EMS EBS ESP, and (ii) revise their configuration management procedure to document the new configuration management tool.

Additionally, URE1 documented the previous installation of the EMS through the use of a Change Control Form. URE1 also included configuration management procedures within its Change Control Procedure. Finally, URE1 updated its Cyber Security Procedures and trained relevant personnel on the revisions.

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.

The UREs' Violations of CIP-004-1 R1 (RFC201100964, RFC2011001276, and RFC2011001277)

The UREs' Mitigation Plan to address their violations of CIP-004-1 R1 was submitted to Reliability*First* stating it had been completed.[45] The Mitigation Plan was accepted by Reliability*First* and approved by NERC.[46] The Mitigation Plan for these violations was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required URE1 to identify all off-site contractors who did not receive the quarterly reinforcement in sound security practices. The UREs developed and implemented a process to ensure that off-site contractors having authorized cyber access to CCAs receive the required quarterly reinforcement in sound security practices.

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.

The UREs' Violations of CIP-004-2 R2 (RFC201100965, RFC2012010075, and RFC2012010076)

URE1's Mitigation Plan to address its violation of CIP-004-2 R2 was submitted to Reliability*First* stating it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC.[47] The Mitigation Plan for RFC201100965 is designated as RFCMIT007197 and was submitted as non-public information to FERC in accordance with FERC orders. URE2 and URE3 submitted a Mitigation Plan to address their violations of CIP-004-2 R2 to Reliability*First* stating it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT007237 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to revoke the involved employee's access rights and reinforce training and PRA requirements through a security awareness campaign.

[45] The Mitigation Plan lists only the URE1 violation ID; however, the UREs submitted an errata sheet correcting this error. In the errata sheet, the UREs list the violation ID numbers for URE2 and URE3.
[46] The Verification of Mitigation Plan Completion states that NERC approved the Mitigation Plan.
[47] The Verification of Mitigation Plan Completion states that NERC approved the Mitigation Plan.

The UREs certified that the above Mitigation Plan requirements were completed.[48] 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.

The UREs' Violations of CIP-004-1 R3 (RFC201100966, RFC2011001278, RFC2011001279)

The UREs' Mitigation Plan to address their violations of CIP-004-1 R3 was submitted to Reliability*First*.[49] The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT006039 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to revise their PRA programs to require updates of PRAs for cause, and to distribute the revised PRA program to relevant personnel.

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.

The UREs' Violations of CIP-004-1 R4 (RFC2011001280, RFC2011001281, RFC2011001282)

The UREs' Mitigation Plan to address their violations of CIP-004-1 R4 was submitted to Reliability*First*. The UREs submitted an amended Mitigation Plan to address the violations of CIP-004-1 R4 to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT007196 and was submitted as non-public information to FERC in accordance with FERC orders**.**

---

[48] Parent Company certified that it completed the Mitigation Plans. Parent Company subsequently submitted a letter to Reliability*First* that Parent Company identified additional instances of noncompliance relating to the implementation of its cyber security training program and determined additional mitigating activities were necessary to achieve compliance with CIP-004-2 R2. Reliability*First* accepted Parent Company's proposed milestone additions and granted Parent Company its requested extension of time to complete additional mitigating activities. The Certification of Mitigation Plan completions were signed and dated. The Verification of Mitigation Plan completion states Parent Company submitted the Certification of Mitigation Plan completions.

[49] Although only the URE1 violation ID is included in the Mitigation Plan, the Mitigation Plan also covers RFC2011001278 and RFC2011001279.

The UREs' Mitigation Plan required the UREs' to revoke access for each of the individuals who no longer required access and updated the user access lists. The UREs revised and implemented their procedures for access controls and account management to clarify the quarterly review and assessment process and ensure compliance with CIP-004. Finally, the UREs trained relevant personnel on the new and revised procedures.

The UREs certified that the above Mitigation Plan requirements were completed.[50] 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.

The UREs' Violations of CIP-005-1 R1 (RFC201100967, RFC2011001178, RFC2011001179)

The UREs' Mitigation Plan to address their violations of CIP-005-1 R1 was submitted to Reliability*First*. The UREs submitted an amended Mitigation Plan to address the violations of CIP-005-1 R1 to Reliability*First.*[51] The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT007198 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan requires the UREs to afford the protective measures specified in each of the CIP Reliability Standards listed in CIP-005-1 R1.5 to Cyber Assets used in the access control and monitoring of the ESP. The UREs updated their processes and procedures related to these Cyber Assets and trained all necessary personnel on the changes. The UREs also revised the documentation of their ESPs, Cyber Assets within the ESPs, electronic access points to the ESPs, and Cyber Assets deployed for the access control and monitoring of these access points. The UREs will file all necessary TFEs for those actions which are not technically feasible.

[50] Parent Company certified that they completed the Mitigation Plan for CIP-004-1, R4. Subsequently, Parent Company submitted a letter to Reliability*First* stating Parent Company determined the Mitigation Plan did not fully address the possible violation identified in the Reliability*First* audit report and additional mitigating actions were necessary to achieve compliance with CIP-004-1, R4. Reliability*First* accepted Parent Company's proposed milestone additions. Parent Company submitted a second letter to Reliability*First* stating that, as disclosed to Reliability*First,* Parent Company identified additional instances of noncompliance with CIP-004-1, R4. Specifically, additional personnel were granted authorized cyber and unescorted physical access to CCAs without completing the required training or having a current PRA on file. Therefore, Parent Company determined further amendments to the Mitigation Plan were necessary to achieve compliance with CIP-004-1, R4. Reliability*First* granted Parent Company its request to further amend the Mitigation Plan associated with CIP-004-1, R4 and Parent Company certified it completed all additional mitigating actions.

[51] The UREs submitted a request to Reliability*First* for additional time to complete additional milestones to address its violation of CIP-005-1 R1. Reliability*First* granted this request.

The UREs' Violations of CIP-005-1 R2 (RFC201100968, RFC2011001283, and RFC2011001284)

The UREs' Mitigation Plan to address their violations of CIP-005-1 R2 was submitted to Reliability*First*. The UREs submitted an amended Mitigation Plan to address the violations of CIP-005-1 R2 to Reliability*First* with different, expected completion dates for URE1, URE2 and URE3. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT007189 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to configure electronic access control devices to display an appropriate use banner on the user screen upon interactive access. The UREs implemented procedures regarding appropriate use banners and the required disabling of non-essential ports and services. Where technically infeasible to implement appropriate use banners, URE2 and URE3 submitted a TFE to Reliability*First* for the devices. URE1 also assessed its ports and services and implemented procedures to ensure that only ports and services required for normal and emergency operations were enabled.

The UREs certified that the above Mitigation Plan requirements were completed.[52] 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.

URE1's Violation of CIP-005-1 R3 (RFC201100969)

URE1's Mitigation Plan to address its violation of CIP-005-1 R3 was submitted to Reliability*First* with an adjusted proposed completion date.[53] The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT006040 and was submitted as non-public information to FERC in accordance with FERC orders**.**

URE1's Mitigation Plan required URE1 to implement a new EMS with associated tools that provide URE1 with the ability to detect and alert for attempted or actual unauthorized access. URE1 updated its procedures for monitoring and logging access, and trained relevant personnel on the procedures. Additionally, URE1 performed the 90-day review of the access logs for each quarter and will implement a monthly review process to ensure logs are accurately captured and reviewed on a going-forward

[52] The Verification of Mitigation Plan completion states that Parent Company certified that it completed the Mitigation Plan.
[53] URE1 submitted a request to Reliability*First* for additional time to complete additional milestones to address its violation of CIP-005-1 R3. Reliability*First* granted this request. The UREs submitted a request to Reliability*First* to complete a different milestone activity under RFCMIT006040. Reliability*First* granted this request.

basis. URE1 will review all ESP access points, Cyber Assets within an ESP, communications links, and monitoring processes.

URE1 certified that the above Mitigation Plan requirements were completed. URE1 submitted evidence of completion of its Mitigation Plan.

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

URE1's Violation of CIP-005-1 R4 (RFC201100970)

URE1's Mitigation Plan to address its violation of CIP-005-1 R4 was submitted to Reliability*First* stating it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT006139 and was submitted as non-public information to FERC in accordance with FERC orders.

URE1's Mitigation Plan required URE1 to conduct a cyber vulnerability assessment, wherein it reviewed controls for default accounts and network management community strings. URE1 implemented a new EMS, which permits URE1 to make necessary modifications to its default accounts and network management strings. Finally, URE1 updated its cyber vulnerability assessment procedure to require a review of all default accounts and network management community strings during all cyber vulnerability assessments.

URE1 certified that the above Mitigation Plan requirements were completed. URE1 submitted evidence of its Mitigation Plan.

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

The UREs' Violations of CIP-005-1 R5 (RFC201100971 RFC2011001285, and RFC2011001286)

The UREs' Mitigation Plan to address their violations of CIP-005-1 R5 was submitted to Reliability*First* stating it had been completed for URE1, URE2 and URE3. The Mitigation Plan was accepted by Reliability*First* and approved by NERC.[54] The Mitigation Plan for these violations is designated as RFCMIT007190 and was submitted as non-public information to FERC in accordance with FERC orders.

[54] The Verification of Mitigation Plan completion states Reliability*First* accepted the Mitigation Plan.

The UREs' Mitigation Plan required the UREs to review and update their documentation to accurately reflect current configurations and processes.

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.

The UREs' Violations of CIP-006-1 R1 (RFC201100972, RFC2011001287, and RFC2011001288)

The UREs' Mitigation Plan to address their violations of CIP-006-1 R1 was submitted to Reliability*First* with an adjusted proposed completion date.[55] The UREs submitted an amended Part B Mitigation Plan and an amended Part A Mitigation Plan to Reliability*First* to address the violations of CIP-006-1 R1.[56] The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007191 and was submitted as non-public information to FERC in accordance with FERC orders.[57]

The UREs' Mitigation Plan required the UREs to amend their physical security plans to include all the information required by the sub-requirements of CIP-006-1 R1 within their physical security plans. The UREs additionally updated their visitor log procedures and documentation to ensure that employees and visitors properly document escorted access. Furthermore, the UREs afforded the protective measures specified in each of the CIP Reliability Standards listed in CIP-006-1 R1.8 to their Cyber Assets used in the access control and monitoring of the PSPs. The UREs updated their processes and

[55] The UREs submitted to Reliability*First* two Mitigation Plans which addressed different components of their violations of CIP-006-1 R1. Reliability*First* classified these two documents as the UREs' CIP-006-1 R1 Mitigation Plan "Part A" and "Part B." Part A addresses the UREs' noncompliance with CIP-006-1 R1.1 R1.2, R1.3, and R1.6. Part B addresses the UREs' noncompliance with CIP-006-1 R1.8.

[56] The UREs submitted a request to Reliability*First* for additional time to complete certain of their milestone activities listed within RFCMIT007191. Reliability*First* granted this request.

[57] Parent Company submitted a request to correct a typographical error on page 11 of 37, Section C3, which incorrectly stated the date when the recovery plan was revised . Three days later, Reliability*First* issued a letter to Parent Company acknowledging the corrected milestone activity completion date. Parent Company submitted a request to Reliability*First* to further revise Mitigation Plan milestone activities for the above-captioned Mitigation Plan. Specifically, Parent Company requested that it may revise CIP-006, R2.2 Corporate IT (CIP-007, R1) Task 5, CIP-006, R2.2 Corporate IT (CIP-007, R5) Task 9, CIP-006, R2.2 Corporate IT (CIP-003, R5) Task 2, and CIP-006, R2.2 Corporate IT (CIP-009, R1 and R4) Tasks 14 and 16. Reliability*First* accepted Parent Company's proposed revisions to the aforementioned Mitigation Plan tasks. Finally, Parent Company submitted a request to correct a clerical error in Task 2.2 in its Mitigation Plan. Reliability*First* granted Parent Company's request to revise the completion date for Task 2.2.

procedures related to these Cyber Assets and trained all necessary personnel on the changes. The UREs filed all necessary TFEs for those actions which are not technically feasible.

The UREs certified that the above Mitigation Plan requirements for Part A were completed and the UREs certified that the above Mitigation Plan requirements for Part B 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.

The UREs' Violations of CIP-007-1 R1 (RFC201100973, RFC2011001289, and RFC2011001290)

The UREs' Mitigation Plan to address its violations of CIP-007-1 R1 was submitted to Reliability*First*. The UREs' submitted an amended Mitigation Plan with a proposed completion date. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT007192 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs' to: revise their test procedures; install firewalls in their test environment; implement their test environment; and ensure that their test environment reflects the production environment. URE2 and URE3 will also implement and commission a new EMS.

The Mitigation Plan also required URE1 to revise its relevant procedures, including its change control procedure and its cyber security testing procedure, and develop and implement new procedures for identifying which cyber security controls to test for new Cyber Assets and changes to existing Cyber Assets within the EMS and EBS ESPs. URE1 additionally installed an automated monitoring tool to test changes to cyber security controls prior to and after installing new Cyber Assets or making significant changes to existing Cyber Assets within its ESPs. Finally, URE1 trained all relevant personnel on these changes.

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.

The UREs' Violations of CIP-007-1 R2 (RFC201000561, RFC201000582, and RFC201000540)

The UREs' Mitigation Plan to address its violations of CIP-007-1 R2 was submitted to Reliability*First*with a completion date . The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT005125 and was submitted as non-public information to FERC in accordance with FERC orders.[58]

The UREs' Mitigation Plan required the UREs to create and implement new procedures to ensure that only those ports and services required for normal and emergency operations are enabled, as well as train relevant personnel on these new procedures. The UREs also assessed ports and services, and disabled those ports and services not required for normal and emergency operations.

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.

The UREs' Violations of CIP-007-1 R2 (RFC2012009913, RFC2012009914, and RFC2012009915)

The UREs' Mitigation Plan to address their violation of CIP-007-1 R2 was submitted to Reliability*First*. The UREs submitted an amended Mitigation Plan stating that it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT007157 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to: upgrade the RTUs and enable only those ports and services required for normal and emergency operations, where technically feasible. Additionally, the UREs submitted the necessary TFEs to Reliability*First*, for those devices on which it is technically infeasible to enable only those ports and services required for normal and emergency operations.

URE1 assessed the missed security patch and updated its security patch management procedure to ensure that URE1 performs and documents patch assessments within 30 calendar days of availability. URE1 assessed all 30 devices that run the operating system to ensure patches are current and retrained relevant personnel on appropriate patch management requirements. Additionally, the UREs implemented a security patch service for the field maintenance laptops.

[58] The Settlement Agreement states that NERC submitted the Mitigation Plan to FERC on July 21, 2011.

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.

The UREs' Violations of CIP-007-1 R3 (RFC201100974, RFC201100975, RFC2011001291, and RFC2011001292)

The UREs' Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to Reliability*First*.[59] The UREs submitted an amended Mitigation Plan with three, different proposed completion dates for URE1, URE2 and URE3. The Mitigation Plan was accepted by Reliability*First* and approved by NERC.[60] The Mitigation Plan for these violations is designated as RFCMIT006142 and was submitted as non-public information to FERC in accordance with FERC orders.

URE1's Mitigation Plan required the UREs to complete the following actions: URE2 and URE3 decommissioned their legacy EMS and commissioned a new EMS, which removed two of the operating systems; URE2 and URE3 also installed security patches for the third operating system.

URE1 assessed the missed security patch and updated its security patch management procedure to ensure that URE1 performs and documents patch assessments within 30 calendar days of availability. URE1 assessed all 30 devices that run the operating system to ensure patches are current and retrained relevant personnel on appropriate patch management requirements. Additionally, the UREs implemented a security patch service for the field maintenance laptops.

Finally, URE1 implemented the compensating measures described in its TFE.

The UREs certified that the above Mitigation Plan requirements were completed.[61] The UREs submitted evidence of completion of their Mitigation Plan.

---

[59] Reliability*First* received three versions of this Mitigation Plan. Reliability*First* received three Versions. Reliability*First* only referenced the initial and final versions of each mitigation plan within the Settlement Agreement.

[60] Parent Company submitted a request to Reliability*First* to further amend the Mitigation Plan associated with Parent Company'sviolations of CIP-007, R3, to include additional milestone activities. Within this request, Parent Company stated that they had determined that additional mitigating actions were necessary to return Parent Company to full compliance with CIP-007, R3. Reliability*First* approved Parent Company'srequest to further amend its Mitigation Plan.

[61] Parent Company certified that they completed the Mitigation Plan for CIP-007-1, R3. Parent Company subsequently submitted a letter to Reliability*First* stating that Parent Company identified four additional instances of noncompliance, which were disclosed to Reliability*First* and determined additional mitigating actions were necessary to achieve compliance with CIP-007-1, R3. Reliability*First* accepted Parent Company's proposed milestone additions.

After Reliability*First*'s review of the UREs' submitted evidence, Reliability*First* verified that the UREs' Mitigation Plan was completed on September 7, 2012.

The UREs' Violations of CIP-007-1 R4 (RFC201100976, RFC2011001293, and RFC2011001294)

The UREs' Mitigation Plan to address its violation of CIP-007-1 R4 was submitted to Reliability*First*. The UREs submitted an amended Mitigation Plan with different proposed completion dates for URE1, URE2 and URE3. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT007193 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to reconfigure their two backup servers so that they were capable of adding new software and installing malware prevention tools and their related signature files. Subsequently, URE2 and URE3 installed malware prevention tools and the related signature files on their two backup servers.

URE1 updated its malicious software prevention procedure to ensure that it tests all anti-virus and malware signatures before applying each signature to the production environment. URE1 also implemented and tested all new anti-virus and malware signatures prior to installing the signatures in the EMS production environment. URE1 documented the technical problems with the software program related to its possible violation of CIP-007-1 R4, revised its procedures, and will train relevant individuals on the revision.

The UREs developed and implemented procedures specific to their substation compliance with CIP-007 R4; trained relevant personnel on these new procedures; and developed test plans to ensure testing is conducted in a separate test environment that reflects the production environment.

The UREs certified that the above Mitigation Plan requirements were completed.[62] The UREs submitted evidence of completion of their Mitigation Plan.

[62] Parent Company certified that they completed the Mitigation Plan for CIP-007-1, R4. Parent Company subsequently submitted a letter to Reliability*First* stating that, as disclosed to Reliability*First,* Parent Companyidentified two additional instances in which Parent Company did not comply with CIP-007-1, R4. Specifically, URE1 EMS was unable to test and install anti-malware patches on certain devices. Therefore, Parent Company determined additional mitigation actions were necessary to achieve compliance with CIP-007-1, R4. Reliability*First* accepted Parent Company's proposed milestone additions and new proposed completion date.

After Reliability*First*'s review of the UREs submitted evidence, Reliability*First* verified that the UREs' Mitigation Plan was completed on July 27, 2012.

The UREs' Violations of CIP-007-1 R5 (RFC201100977, RFC2011001180, and RFC2011001181)

The UREs' Mitigation Plan to address their violation of CIP-007-1 R5 was submitted to Reliability*First* with different proposed completion dates for URE1, URE2 and URE3.[63] The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT006145 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to complete the following actions: a) URE2 and URE3 decommissioned their legacy EMS and implemented a new EMS which allowed URE2 and URE3 to change default account passwords; b) URE2 and URE3 utilized log books to manually maintain an audit trail of account use for their shared account on the EMS console; and c) URE2 and URE3 filed a TFE for those devices on which they cannot use technical measures to enforce password complexity.

URE1 installed an automated monitoring tool to monitor Cyber Assets in the EMS and EBS ESPs and will train staff on this automated tool. URE1 updated its procedures and documentation to implement process changes, including its EMS security and access monitoring procedure, cyber security event monitoring guideline, and EMS cyber security event monitoring matrix. URE1 implemented its procedural controls regarding the frequency for changing passwords for its Cyber Assets within the EMS and EBS ESPs. URE1 changed the password of an asset at its Critical Asset substation and developed and implemented a procedure and a form to ensure password complexity and train relevant personnel on these changes

The UREs certified that the above Mitigation Plan requirements were completed.[64] The UREs submitted evidence of completion of their Mitigation Plan.

[63] The Mitigation Plan submittal form. The UREs submitted a request to Reliability*First* to complete an additional milestone to mitigate URE2's violation of CIP-007-1 R5. Reliability*First* granted this request.

[64] Parent Company certified that they completed the Mitigation Plan for CIP-007-1, R5. Parent Company subsequently submitted a letter to Reliability*First* stating that Parent Company identified three additional instances in which Parent Company did not comply with the password requirements specified in CIP-007, R5.3 and therefore, additional mitigating actions were necessary to achieve compliance with CIP-007-1, R5. Reliability*First* accepted Parent Company's proposed milestone additions and granted Parent Company's request for extension of Mitigation Plan completion.

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

URE1's Violation of CIP-007-1 R5 (RFC201100978)

URE1's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to Reliability*First*. The URE1 submitted an amended Mitigation Plan stating it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT007200 and was submitted as non-public information to FERC in accordance with FERC orders.

URE1's Mitigation Plan required URE1 to create and implemented a form for password changes on the server to certify that the changed password consists of a password compliant with CIP-007-1 R5.3. URE1 also updated its procedures to expand the review process and criteria for password complexity, trained relevant personnel on the new procedure, and changed the password on the server to meet the requirements of CIP-007-1 R5.

URE1 certified that the above Mitigation Plan requirements were completed. URE1 submitted evidence of completion of its Mitigation Plan.

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

The UREs' Violations of CIP-007-1 R6 (RFC201100979, RFC2011001295, and RFC2011001296)

The UREs' Mitigation Plan to address their violation of CIP-007-1 R6 was submitted to Reliability*First*. The UREs submitted an amended Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC.[65] The Mitigation Plan for these violations is designated as RFCMIT007194 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to take the following actions: a) URE2 and URE3 reconfigured the CCAs to maintain logs of system events related to cyber security; b) URE1 implemented automated tools and revised its organization processes and procedures to ensure it

[65] Parent Company submitted a request to Reliability*First* to correct task 6 in its Mitigation Plan associated with Parent Company's violations of CIP-007 R3. Within this request, Parent Company stated the change was necessary to correct a clerical error made while drafting the Mitigation Plan milestone completion dates listed on page 10 of the Mitigation Plan. Reliability*First* approved Parent Company's request to revise the completion date for task 6 in the Mitigation Plan.

monitors system events related to cyber security, and trained relevant personnel on these changes; c) the UREs developed, implemented, and trained relevant staff members on procedures to ensure that they monitor electronic access and security status; and d) the UREs also filed TFEs with Reliability*First* for devices that cannot monitor system events related to cyber security.

The UREs certified that the above Mitigation Plan requirements were completed.[66] 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.

URE1's Violation of CIP-007-1 R8 (RFC201100981)

URE1's Mitigation Plan to address its violation of CIP-007-1 R8 was submitted to Reliability*First* stating it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT006042 and was submitted as non-public information to FERC in accordance with FERC orders.

URE1's Mitigation Plan required URE1 to:

1. Review the controls for default accounts during its annual cyber vulnerability assessment;
2. Retire the legacy EMS system that would not permit changes to default accounts;
3. Implement a new EMS that allows for changes to default accounts; and
4. Update its cyber vulnerability procedures to include instructions for reviewing default accounts.

URE1 certified in its Mitigation Plan submitted that the above Mitigation Plan requirements were completed.[67] URE1 submitted evidence of completion of its Mitigation Plan.

[66] Parent Company certified that they completed the Mitigation Plan for CIP-007-1, R6. Parent Company subsequently submitted a letter to Reliability*First* stating that Parent Company discovered eight additional switches that cannot perform the required security status monitoring and therefore, additional mitigation actions were necessary to achieve compliance with CIP-007-1, R6. Reliability*First* accepted Parent Company's proposed milestone additions and granted Parent Company its requested extension.

[67] URE1 also submitted a formal Certification of Mitigation Plan Completion stating that it completed its Mitigation Plan.

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

The UREs' Violations of CIP-008-1 R1 RFC201100982, RFC2011001182, and RFC2011001183)

The UREs' Mitigation Plan to address their violations of CIP-008-1 R1 was submitted to Reliability*First*. The UREs submitted an amended Mitigation Plan with separate, proposed completion dates for URE2 and URE3. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT006519 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required URE2 and URE3 to conduct an annual test of their Cyber Security Incident response plans. The UREs' Mitigation Plan required URE1 to: 1) revise its Cyber Security Incident response plan to address procedures to characterize and classify events; 2) list the response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans; and 3) identify the process for reporting Cyber Security Incidents to the ESISAC. URE1 also trained relevant personnel on the updated response plan.

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.

The UREs' Violations of CIP-009-1 R1 (RFC201100983, RFC2011001184, and RFC2011001185)

The UREs' Mitigation Plan to address their violations of CIP-009-1 R1 was submitted to Reliability*First*. The UREs submitted an amended Mitigation Plan for URE2 and URE3 and URE1.[68] The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT006520 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required URE2 and URE3 to revise their recovery plan procedures to list the required actions to restore individual assets into normal operating conditions. The UREs' Mitigation Plan required URE1 to revise its EMS CCA restoration procedure to include detailed recovery plans for

[68] UREs submitted a request to Reliability*First* for additional time to complete a milestone to mitigate their Alleged Violations of CIP-009-1 R1. Reliability*First* granted this request.

CCAs and Cyber Assets within the new EMS ESP. URE1 also retired its legacy EMS and implemented the new EMS. URE1 revised its recovery plan for substation CCAs to list required actions to respond to events or conditions of varying duration and severity that would activate the recovery plan, and defined the roles and responsibilities of responders. Finally, URE1 conducted an exercise of its recovery plan.

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.

URE1's Violation of CIP-009-1 R2 (RFC201100984)

URE1's Mitigation Plan to address its violation of CIP-009-1 R2 was submitted to Reliability*First*. URE1 submitted an amended Mitigation Plan stating that it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT006521 and was submitted as non-public information to FERC in accordance with FERC orders.

URE1's Mitigation Plan required URE1 to revise its EMS CCAs restoration procedure to include a recovery plan, including a provision requiring the annual exercise of the recovery plan. Additionally, URE1 performed recovery exercises as defined within its recovery plan.

URE1 certified in its Mitigation Plan that that the above Mitigation Plan requirements were completed.[69] 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.

URE1's Violation of CIP-009-1 R3 (RFC201100985)

URE1's Mitigation Plan to address its violation of CIP-009-1 R3 was submitted to Reliability*First* stating that it had been completed.[70] The Mitigation Plan was accepted by Reliability*First* and approved by

[69] URE1 also submitted a formal Certification of Mitigation Plan Completion stating that it completed its Mitigation Plan.
[70] The Mitigation Plan submittal form.

NERC. The Mitigation Plan for these violations is designated as RFCMIT006522 and was submitted as non-public information to FERC in accordance with FERC orders.

URE1's Mitigation Plan required URE1 to conduct an exercise of its recovery plan, update the procedures within which its recovery plan is contained, and notify appropriate personnel of the changes to the recovery plan.

URE1 certified in its Mitigation Plan that the above Mitigation Plan requirements were completed.[71] 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.

The UREs' Violations of CIP-009-1 R4 (RFC201100986, RFC2011001299, and RFC2011001300)

The UREs' Mitigation Plan to address their violations of CIP-009-1 R4 was submitted to Reliability*First*. The UREs submitted an amended Mitigation Plan for URE2 and URE3 and URE1.[72] The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT007195 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to update their recovery plans to include the backup and restoration procedures as a component of the recovery plan. URE1 conducted an exercise of its recovery plan to test its processes and procedures for the backup and storage of information required to successfully restore its Critical Cyber Assets. URE1 implemented additional revisions to its recovery plan and communicated all changes to necessary personnel.

URE2 and URE3 implemented a new EMS, revised their backup and restoration procedures to reflect the new EMS, conducted a backup and restore of a CCA within the new EMS, and revised their backup and restore procedures as needed.

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

[71] URE1 also submitted a formal Certification of Mitigation Plan Completion stating that it completed its Mitigation Plan.
[72] The UREs submitted a request to Reliability*First* to revise a milestone listed within RFCMIT007195. Reliability*First* granted this request.

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

The UREs' Violations of CIP-009-1 R5 (RFC201100987, RFC2011001186, and RFC2011001187)

The UREs' Mitigation Plan to address their violations of CIP-009-1 R5 was submitted to Reliability*First*. The UREs submitted an amended Mitigation Plan stating that it had been completed for URE1 URE2 and URE3. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT006533 and was submitted as non-public information to FERC in accordance with FERC orders.

The UREs' Mitigation Plan required the UREs to revise their backup and restoration procedures to include the testing of backup media. The UREs also conducted testing of the backup media for the devices which they had previously failed to provide backup testing information.

The UREs certified in its Mitigation Plan that the above Mitigation Plan requirements were completed.[73] 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.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[74]

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,[75] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on August 14, 2012. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of a seven hundred twenty-five thousand dollars ($725,000) 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

[73] URE1 also submitted a formal Certification of Mitigation Plan Completion stating that it completed its Mitigation Plan.
[74] *See* 18 C.F.R. § 39.7(d)(4).
[75] *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).

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. Certain of the violations constituted the UREs' repeat occurrences of violations of the subject NERC Reliability Standards, as discussed above;
2. the UREs self-reported some of the violations;[76]
3. Reliability*First* reported that the UREs were cooperative throughout the compliance enforcement process;
4. Reliability*First* considered the UREs' lack of a culture of compliance regarding the CIP Reliability Standards at the time Reliability*First* discovered the violations at issue in this Agreement. Reliability*First* determined that the UREs had a lack of familiarity with their CIP processes and procedures and a failure to implement those processes and procedures. Additionally, Reliability*First* noted that responsibility for compliance with CIP Reliability Standards at the UREs was spread among six separate executives, thereby reducing ownership of the compliance processes and causing inconsistent application of these processes;
5. Reliability*First* considered the UREs' subsequent strides toward fostering a culture of compliance following the discovery of the violations. Upon discovering the violations, the UREs immediately began working with Reliability*First* to remedy the violations and to create an improved compliance program going forward;
6. The UREs' collaboration with Reliability*First* was evidenced through the UREs' participation in numerous in-person meetings and conference calls with Reliability*First* personnel. For example, Reliability*First* executives engaged executives of the UREs to ensure the UREs' organizational commitment to address the violations. During a separate meeting, the UREs presented their compliance initiative to Reliability*First* personnel and solicited Reliability*First*'s feedback regarding their progress in returning to compliance with the CIP Reliability Standards. Additionally, the UREs completed weekly conference calls with Reliability*First* personnel to discuss the ongoing progress of mitigating activities;
7. Through these interactions, the UREs demonstrated a willingness to collaborate with Reliability*First* in order to maximize the reliability benefits associated with Reliability*First*'s

[76] RFC201100964, RFC201100965, RFC201100969, RFC201100970, RFC201100973, RFC201100981, RFC201100985, RFC201100987, RFC2011001276, RFC2011001277, RFC2012010075, RFC2012010076, RFC2011001283, RFC2011001284, RFC2011001289, RFC2011001290, RFC201000561, RFC201000582, RFC201000540, RFC2012009913, RFC2012009914, RFC2012009915, RFC2011001293, and RFC2011001294 received self-reporting credit.

CMEP activities. For these reasons, Reliability*First* considered the UREs' overall cooperation with Reliability*First* during the enforcement process to constitute a mitigating factor for penalty purposes;

8. The UREs also implemented a compliance initiative aimed at restructuring departments and personnel to enforce compliance with Reliability Standards, refocusing senior management leadership toward compliance activities, standardizing compliance procedures, monitoring mitigation activities, and implementing controls to ensure future compliance. For the reasons discussed below, Reliability*First* considered the UREs' implementation of the compliance initiative to warrant mitigating credit for penalty purposes;

9. Within this compliance initiative, the UREs expanded their compliance staff and enhanced their compliance roles and responsibilities. The UREs created the position of CCO, who is responsible for leading Parent Company's Corporate Compliance organization and corporate compliance efforts, including with respect to NERC compliance efforts. The CCO works closely with senior management, including directly reporting to the Senior Vice President and General Counsel and having access to the Audit Committee of the Board of Directors. The CCO also works closely with subject matter experts in relevant departments to develop and advance a culture of compliance built upon the implementation of rigorous subject area compliance plans;

10. Additionally, the UREs identified Executive Standards Owners for each CIP Reliability Standard to maintain an active and visible role in supervising compliance, participating in a NERC Steering Committee, and overseeing the completion of compliance tasks by personnel across the UREs. Furthermore, the UREs filled the designated compliance positions of Standards Managers, who are responsible for ensuring that key tasks are assigned, tracked, and completed on a timely basis, and are critical to the UREs' ongoing compliance efforts;

11. Within the Parent Company Compliance Department, the UREs also added a position of Compliance Manager to handle Cyber Security and routinely meet with Standards Managers to plan for continuous improvement goals, self-certification strategy, annual internal reviews of tasks and spot checks, and annual risk analysis. Within the same department, the UREs also added a position of Principal Consultant to manage compliance enforcement correspondence between both Cyber Security and Operations & Planning NERC Compliance. The UREs have structured additional measures and timelines to hire additional full time employees identified by the compliance initiative;

12. In addition to the hiring of personnel and restructuring of roles and responsibilities, the UREs have included other activities within their compliance initiative to promote and foster their improved culture of compliance. The UREs are unifying their corporate procedures to ensure the standardization of procedures, processes, and other documents, which will ensure compliance across functional areas of each of the UREs;

13. The UREs are also in the process of changing their manual compliance forms into an automated online system of forms and workflows in an effort to standardize fields and forms, expedite workflows, and improve document accuracy and completeness, version control, and document storage and retrieval.
14. The UREs are in the process of building an intelligence network to connect key substations which will increase the UREs' physical security by facilitating physical access monitoring and surveillance, providing video enhancing physical security forensics, enhancing physical security at unmanned facilities, and increasing efficiencies in the badge process for remote sites;
15. There was no evidence of any attempt to conceal a violation or evidence of any intent to do so;
16. Reliability*First* determined that the violations, when viewed collectively, did pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
17. 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 seven hundred twenty-five thousand dollars ($725,000) 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. The public release of this information could compromise system security due to its inclusion of information regarding: the identification of the types and classes of vulnerabilities that this entity (and all entities) must continuously guard against; the detailed mitigating measures this entity took or continues to take to remedy those vulnerabilities that serve as its vulnerability defense plan; security assessments and root cause analyses; a description of system architecture and configuration,

facilities, and other assets that, if disclosed, would assist in the planning of a targeted, vectored attack; and other sensitive data.

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, included as Attachment a;

1. URE1's Mitigation Plan designated as RFCMIT-00-6035, included as attachment A to the Settlement Agreement;
2. URE1's Mitigation Plan designated as RFCMIT-00-6036, included as attachment B to the Settlement Agreement;
3. URE1's amended Mitigation Plan designated as RFCMIT-00-6136;
4. URE1's amended Mitigation Plan designated as RFCMIT006137;
5. URE1's Mitigation Plan designated as RFCMIT006037;
6. URE1's amended Mitigation Plan designated as RFCMIT006517;
7. UREs' amended Mitigation Plan designated as RFCMIT007188;
8. UREs' Mitigation Plan designated as RFCMIT006038;
9. URE1's Mitigation Plan designated as RFCMIT007197;
10. URE2 and URE3's Mitigation Plan designated as RFCMIT007237;
11. UREs' Mitigation Plan designated as RFCMIT006039;
12. UREs' amended Mitigation Plan designated as RFCMIT007196;
13. Request to Supplement Mitigation Plan - NERC Violation ID Nos. RFC201100967, RFC2011001178, and RFC2011001179; included as attachment M to the Settlement Agreement;

14. Reliability*First*'s Approval of Request to Supplement Mitigation Plan RFCMIT007198; included as attachment N to the Settlement Agreement;
15. UREs' amended Mitigation Plan designated as RFCMIT007198;
16. UREs' amended Mitigation Plan designated as RFCMIT007189;
17. Request for Additional Time to Complete Additional Milestones under NERC Mitigation Plan ID No. RFCMIT006040;
18. Approval of Request for Additional Time to Complete Additional Milestones under NERC Mitigation Plan ID No. RFCMIT006040;
19. Request to Supplement Mitigation Plan - NERC Mitigation Plan ID No. RFCMIT6040;
20. Reliability*First*'s Approval of Request to Supplement Mitigation Plan - NERC Mitigation Plan ID No. RFCMIT6040;
21. URE1's Mitigation Plan designated as RFCMIT006040;
22. URE1's Mitigation Plan designated as RFCMIT006139;
23. UREs' Mitigation Plan designated as RFCMIT007190;
24. Request to Supplement Mitigation Plan - NERC Violation ID Nos. RFC201100972, RFC2011001287, and RFC2011001288;
25. Reliability*First*'s Approval of Request to Supplement Mitigation Plan RFCMIT007191;
26. UREs' amended Mitigation Plan designated as RFCMIT007191;
27. UREs' amended Mitigation Plan designated as RFCMIT007192;
28. UREs' Mitigation Plan designated as RFCMIT007157;
29. UREs' amended Mitigation Plan for CIP-007-1 R2;
30. Request to Supplement Mitigation Plan - NERC Violation ID Nos. RFC201100974, RFC201100975, RFC2011001291, and RFC2011001292;
31. Reliability First's Approval of Request to Supplement Mitigation Plan - NERC Violation ID Nos. RFC201100974, RFC201100975, RFC2011001291, and RFC2011001292;
32. UREs' amended Mitigation Plan designated as RFCMIT006142;
33. TFE Request;
34. UREs' amended Mitigation Plan designated as RFCMIT007193;

35. Request for Additional Time to Complete Additional Milestones under NERC Mitigation Plan ID No. RFCMIT006145;
36. Approval of Request for Additional Time to Complete Additional Milestones under NERC Mitigation Plan ID No. RFCMIT006145;
37. UREs' Mitigation Plan designated as RFCMIT006145;
38. URE1's amended Mitigation Plan designated as RFCMIT007200;
39. UREs' amended Mitigation Plan designated as RFCMIT007194;
40. URE1's Mitigation Plan designated as RFCMIT006042;
41. UREs' amended Mitigation Plan designated as RFCMIT006519;
42. Request for Additional Time under NERC Violation ID Nos. RFC201100983, RFC2011001184, and RFC2011001185;
43. Approval of Request for Additional Time under NERC Violation ID Nos. RFC201100983, RFC2011001184, and RFC2011001185;
44. UREs' amended Mitigation Plan designated as RFCMIT006520;
45. URE1's amended Mitigation Plan designated as RFCMIT006521;
46. URE1's Mitigation Plan designated as RFCMIT006522;
47. Request to Supplement Mitigation Plan - NERC Violation ID Nos. RFC201100986, RFC2011001299, and RFC2011001300;
48. Reliability*First*'s Approval of Request to Supplement Mitigation Plan RFCMIT007195;
49. UREs' amended Mitigation Plan designated as RFCMIT007195;
50. UREs' amended Mitigation Plan designated as RFCMIT006533;

b) UREs Self-Report form for the violations of CIP-007-1 R2.1, 2.2, included as Attachment b;

c) URE1's Self-Report Form for the violations of CIP-003-1 R5, CIP-004-1 R1,CIP-004-2 R2, R4, CIP-005-1 R1, R3, CIP-006-1b R1, R2, CIP-007-1 R1, R4, R5, R8, CIP-007-3 R3, R6, CIP-009-1 R1, R2, R3, R5, included as Attachment c;

d) URE1's source document for the violations of CIP-002-1 R1, R2, R3, R4, CIP-002-2 R1, R2, R3, R4, CIP-002-3 R1, R2, R3, R4, CIP-003-1 R1, R5, R6, CIP-003-2 R1, R5, R6, CIP-003-3 R1, R5, R6, CIP-004-1 R3, CIP-004-2 R3, CIP-004-3 R3, R4, CIP-005-1 R1, R2, R5, CIP-005-2 R1, R2, R5, CIP-005-3 R1, R2, R5, CIP-006-1 R1, CIP-006-2 R1, CIP-006-3 R1, CIP-007-1 R2, R3, R4, R5, R6, CIP-007-2 R2, R3, R4, R5, R6,

CIP-007-3 R2, R3, R4, R5, R6, CIP-008-1 R1, CIP-008-2 R1, CIP-008-3 R1, CIP-009-1 R1, R2, R4, CIP-009-2 R1,R2, R4, CIP-009-3 R1, R2, R4, included as Attachment d;

e) URE2 and URE3's Self-Report form for the violations of CIP-004-1R1, R4, CIP-005-1 R1, R2, R3, R4, CIP-006-1b R2, CIP-009-1 R1, R2, R4, CIP-007-1 R1, R2, R3, R4, R5, R7, CIP-009-1 R1, R2, R4, included as Attachment e;

f) URE2 and URE3's source document for the violations of CIP-004-2 R4, CIP-004-3 R4, CIP-005-1 R1, CIP-005-2 R1, CIP-005-3 R1, CIP-007-3 R5, CIP-008-1 R1, CIP-008-2 R1, CIP-008-3 R1, CIP-009-1 R1, R5, CIP-009-2 R1, R5, CIP-009-3 R1, R5, included as Attachment f;

g) Record documents for the violation of CIP-002-1 R1, included as Attachment g:

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

h) Record documents for the violation of CIP-002-1 R2, included as Attachment h:

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

i) Record documents for the violation of CIP-002-1 R3, included as Attachment i:

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

j) Record documents for the violation of CIP-002-1 R4, included as Attachment j:

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

k) Record documents for the violation of CIP-003-1 R1, included as Attachment k:

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

l) Record documents for the violation of CIP-003-1 R5, included as Attachment l:

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

m) Record documents for the violation of CIP-003-1 R6, included as Attachment m:

1. UREs' Certification of Mitigation Plan Completion;

2. Reliability*First*'s Verification of Mitigation Plan Completion;

n) Record documents for the violation of CIP-004-1 R1, included as Attachment n:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

o) Record documents for the violation of CIP-004-2 R2, included as Attachment o:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

p) Record documents for the violation of CIP-004-1 R3, included as Attachment p:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

q) Record documents for the violation of CIP-004-1 R4, included as Attachment q:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

r) Record documents for the violation of CIP-005-1 R2, included as Attachment r:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

s) Record documents for the violation of CIP-005-1 R3, included as Attachment s:

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

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

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

u) Record documents for the violation of CIP-005-1 R5, included as Attachment u:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

v) Reliability*First*'s Verification Record documents for the violation of CIP-006-1 R1, included as Attachment v:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

w) Reliability*First*'s Verification Record documents for the violation of CIP-007-1 R1, included as Attachment w:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

x) Reliability*First*'s Verification Record documents for the violation of CIP-007-1 R2, included as Attachment x:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

y) Reliability*First*'s Verification Record documents for the violation of CIP-007-1 R3, included as Attachment y:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

z) Reliability*First*'s Verification Record documents for the violation of CIP-007-1 R4, included as Attachment z:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

aa) Reliability*First*'s Verification Record documents for the violation of CIP-007-1 R5, included as Attachment aa:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

bb) Reliability*First*'s Verification Record documents for the violation of CIP-007-1 R5, included as Attachment bb:

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

cc) Reliability*First*'s Verification Record documents for the violation of CIP-007-1 R6, included as Attachment cc:

1. UREs' Certification of Mitigation Plan Completion;

2. Reliability*First*'s Verification of Mitigation Plan Completion;

dd) Reliability*First*'s Verification Record documents for the violation of CIP-007-1 R8, included as Attachment dd:

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

ee) Reliability*First*'s Verification Record documents for the violation of CIP-008-1 R1, included as Attachment ee:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

ff) Reliability*First*'s Verification Record documents for the violation of CIP-009-1 R1, included as Attachment ff:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

gg) Reliability*First*'s Verification Record documents for the violation of CIP-009-1 R2, included as Attachment gg:

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

hh) Reliability*First*'s Verification Record documents for the violation of CIP-009-1 R3, included as Attachment hh:

1. URE1's Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

ii) Reliability*First*'s Verification Record documents for the violation of CIP-009-1 R4, included as Attachment ii:

1. UREs' Certification of Mitigation Plan Completion;
2. Reliability*First*'s Verification of Mitigation Plan Completion;

jj) Reliability*First*'s Verification Record documents for the violation of CIP-009-1 R5, included as Attachment jj:

1. UREs' Certification of Mitigation Plan Completion; and
3. Reliability*First*'s Verification of Mitigation Plan Completion.

A Form of *Notic*e Suitable for Publication[77]

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

[77] *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	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça* Attorney North American Electric Reliability Corporation 1325 G Street, N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net *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.

Megan E. Gambrel* Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 megan.gambrel@rfirst.org	

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

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

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Sonia C. Mendonça
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

cc: The UREs
ReliabilityFirst Corporation

Attachments