

April 30, 2020

**VIA ELECTRONIC FILING**

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

Re: **NERC Full Notice of Penalty regarding [REDACTED]  
FERC Docket No. NP20-\_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty<sup>1</sup> regarding [REDACTED] (and referred to herein as the Entity), NERC Registry ID# [REDACTED]<sup>2</sup> 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)).<sup>3</sup>

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,<sup>4</sup> with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and the Entity have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the violations of the CIP Reliability Standards listed below.

According to the Settlement Agreement, the Entity admits to the violations, and has agreed to the assessed penalty of four hundred fifty thousand dollars (\$450,000).

<sup>1</sup> *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 (2017). *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).

<sup>2</sup> The Entity was included on the NERC Compliance Registry as a [REDACTED]

<sup>3</sup> See 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

<sup>4</sup> For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 2

### **Statement of Findings Underlying the Violations**

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between ReliabilityFirst and the Entity. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2019), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 3

Violation(s) Determined and Discovery Method								
*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation								
NERC Violation ID	Standard	Req.	VRF/VSL	Applicable Function(s)	Discovery Method*	Violation Start-End Date	Risk	Penalty Amount
RFC2017018708	CIP-002-5.1	R1	High/Lower	[REDACTED]	SR	[REDACTED]	Minimal	\$450k
RFC2017017778	CIP-004-6	R2	Lower/Lower	[REDACTED]	SR	[REDACTED]	Minimal	
RFC2017017568	CIP-004-6	R4	Medium/Severe	[REDACTED]	SR	[REDACTED]	Minimal	
RFC2017018261	CIP-004-6	R4	Medium/Severe	[REDACTED]	SR	[REDACTED]	Minimal	
RFC2017018760	CIP-004-6	R4	Medium/Severe	[REDACTED]	SR	[REDACTED]	Moderate	
RFC2017017152	CIP-004-6	R5	Medium/Lower	[REDACTED]	SR	[REDACTED]	Minimal	
RFC2018019570	CIP-005-5	R2	Medium/Moderate	[REDACTED]	SR	[REDACTED]	Moderate	
RFC2017017304	CIP-006-6	R1	Medium/Severe	[REDACTED]	SR	[REDACTED]	Moderate	
RFC2017017547	CIP-006-6	R1	Medium/Severe	[REDACTED]	SR	[REDACTED]	Minimal	
RFC2017018166	CIP-006-6	R1	Medium/Severe	[REDACTED]	SR	[REDACTED]	Minimal	
RFC2017018857	CIP-006-6	R1	Medium/Severe	[REDACTED]	SR	[REDACTED]	Minimal	
RFC2016016341	CIP-007-3a	R3	Lower/Severe	[REDACTED]	SR	[REDACTED]	Moderate	
RFC2016016342	CIP-007-3a	R3	Lower/Severe	[REDACTED]	SR	[REDACTED]	Serious	
RFC2016016343	CIP-007-6	R2	Medium/High	[REDACTED]	SR	[REDACTED]	Minimal	
RFC2017017777	CIP-007-6	R2	Medium/Moderate	[REDACTED]	SR	[REDACTED]	Minimal	
RFC2017017839	CIP-007-6	R2	Medium/Lower	[REDACTED]	SR	[REDACTED]	Minimal	
RFC2018020386	CIP-007-6	R2	Medium/Moderate	[REDACTED]	SR	[REDACTED]	Minimal	

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 4

NERC Violation ID	Standard	Req.	VRF/VSL	Applicable Function(s)	Discovery Method*	Violation Start-End Date	Risk	Penalty Amount
RFC2017017548	CIP-007-6	R4	Medium/ Severe		SR [REDACTED]	[REDACTED]	Serious	\$450k
RFC2018019469	CIP-007-6	R4	Medium/ High		SR [REDACTED]	[REDACTED]	Moderate	
RFC2018020086	CIP-007-6	R4	Medium/ High		SR [REDACTED]	[REDACTED]	Moderate	
RFC2019021564	CIP-007-6	R4	Medium/ Severe		SR [REDACTED]	[REDACTED]	Moderate	
RFC2017016888	CIP-007-6	R5	Medium/ Severe		SR [REDACTED]	[REDACTED]	Minimal	
RFC2016016384	CIP-009-6	R1	Medium/ Severe		SR [REDACTED]	[REDACTED]	Minimal	
RFC2017017546	CIP-010-2	R1; 1.1	Medium/ Severe		SR [REDACTED]	[REDACTED]	Moderate	
RFC2017017765	CIP-010-2	R1	Medium/ Severe		SR [REDACTED]	[REDACTED]	Moderate	
RFC2017017840	CIP-010-2	R1	Medium/ Severe		SR [REDACTED]	[REDACTED]	Minimal	
RFC2017018307	CIP-010-2	R1	Medium/ Severe		SR [REDACTED]	[REDACTED]	Minimal	
RFC2018019647	CIP-010-2	R1	Medium/ Severe		SR [REDACTED]	[REDACTED]	Moderate	
RFC2017017836	CIP-010-2	R3	Medium/ Severe		SR [REDACTED]	[REDACTED]	Moderate	
RFC2017018498	CIP-010-2	R3	Medium/ Severe		SR [REDACTED]	[REDACTED]	Minimal	
RFC2018019048	CIP-010-2	R3	Medium/ Moderate		SR [REDACTED]	[REDACTED]	Minimal	
RFC2017018285	CIP-010-2	R4	Medium/ Severe		SR [REDACTED]	[REDACTED]	Minimal	
RFC2017018761	CIP-010-2	R4	Medium/ Severe		SR [REDACTED]	[REDACTED]	Minimal	
RFC2017017838	CIP-011-2	R1	Medium/ Severe		SR [REDACTED]	[REDACTED]	Minimal	

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 5

### Background to the Violations

[REDACTED]

[REDACTED]

[REDACTED] ReliabilityFirst required and verified that the Entity mitigate the violations as they were being submitted. However, ReliabilityFirst held many of the violations for processing so that it could fully understand and evaluate the scope of the violations and [REDACTED]

The current Settlement Agreement resolves 34 violations of the CIP Reliability Standards [REDACTED]

[REDACTED] The violations resolved in this Settlement Agreement are mostly the result of a combination of contributing causes including: issues implementing new assets, tools, and processes; inadequate training of staff; unclear or overlapping responsibilities; inadequate planning; and gaps in existing processes, procedures, and work instructions. Many of the violations resolved in this Settlement Agreement posed only a minimal risk and could have been Compliance Exceptions under different circumstances, but ReliabilityFirst wanted to consider and evaluate the full scope of [REDACTED]

[REDACTED] Accordingly, the minimal risk violations included in the Settlement Agreement did not materially affect the overall penalty. The penalty in this case is largely based on the two serious risk violations and the moderate risk violations.

The violations resolved in this case do not involve, and are not indicative of, programmatic issues across the Entity's CIP compliance program. The Entity identified many of the violations through internal

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 6

controls that it implemented [REDACTED] Many of the violations were relatively short in duration. ReliabilityFirst expects that the problems associated with the longer duration violations should occur less frequently as the Entity's compliance program continues to mature.

CIP-002-5.1 R1

RFC2017018708

ReliabilityFirst determined that the Entity incorrectly categorized its [REDACTED]

The root cause of this violation was a lack of sufficient controls to [REDACTED]

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the bulk power system (BPS). Attachment 2a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 2b.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 2c and 2d provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

CIP-004-6 R2

RFC2017017778

ReliabilityFirst determined that the Entity's employee had physical access to an applicable Cyber Asset prior to completing required training.

The root cause of this violation was inadequate training and instruction.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 7

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 3a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 3b.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 3c and 3d provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

CIP-004-6 R4

RFC2017017568

ReliabilityFirst determined that the Entity's employees did not follow the Entity's established process for vendors to obtain remote access to the Entity's [REDACTED]

The cause of this violation was a failure to follow established procedures and processes and insufficient workforce management.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 4a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 4b.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 4c and 4d provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017018261

ReliabilityFirst determined that [REDACTED] Entity employees had access to BES Cyber System Information (BCSI) without corresponding authorization records.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 8

The cause of this violation was a failure to implement sufficient controls, processes, and procedures.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 4e includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 4f.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 4g and 4h provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017018760

ReliabilityFirst determined that six of the Entity's employees had access to a shared drive holding BCSI without corresponding authorization records.

The root causes were ineffective controls, processes, and procedures; and insufficient training.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS. Attachment 4i includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 4j.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 4k and 4l provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

CIP-004-6 R5

RFC2017017152



NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 9

ReliabilityFirst determined that the Entity was in violation of CIP-004-6 R5 in two instances. In the first instance, the Entity did not initiate removal of the remote access capabilities of a security contractor's employee within 24 hours of said person's resignation. In the second instance, the Entity failed to change a password for a shared account within 30 days after an employee who knew the password to the account voluntarily resigned.

The causes of this violation were insufficient management and training.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 5a and 5b include the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 5c.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 5d and 5e provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

#### CIP-005-5 R2

RFC2018019570

ReliabilityFirst determined that the Entity had a group on a jump server that did not require multi-factor authentication to gain access to an ESP [REDACTED].

The causes of the violation were inadequate planning and administrative oversight.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS. Attachment 6a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 6b.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 10

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 6c and 6d provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

CIP-006-6 R1

RFC2017017304

ReliabilityFirst determined that the Entity violated CIP-006-6 R1 in three instances. All three instances involved doors that were able to be opened regardless of an individual's previously assigned access privileges.

The causes of this violation were insufficient training and defective equipment.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS. Attachment 7a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 7b.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 7c and 7d provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017017547

ReliabilityFirst determined that during testing, alarms were not triggered when a [REDACTED] door was forced or propped open. The failures were documented on an inspection form, but the contract security personnel failed to create a maintenance ticket and activate and maintain alternate security measures until repairs and retesting were complete.

The cause of this violation was faulty wiring. The issue persisted due to the fact that the Entity's contract security personnel failed to follow established processes and procedures.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 11

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 7e includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 7f.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that ReliabilityFirst had completed all mitigation activities as of [REDACTED]. Attachments 7g and 7h provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017018166

ReliabilityFirst determined that the Entity was in violation of CIP-006-6 R1. [REDACTED]

The cause of this violation was insufficient planning and oversight of the construction project. The Entity's construction project management team did not evaluate whether the project would impact PSPs.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 7i includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 7j.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 7k and 7l provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017018857

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 12

ReliabilityFirst determined that the Entity violated CIP-006-6 R1. The Entity's employee who had unescorted physical access privileges into a particular PSP entered said PSP through a locked door. The physical access control for the PSP was malfunctioning. The card reader denied the employee's access because it read the wrong card. The employee did not realize that access was denied and was able to open the door despite being denied access.

The cause of this violation was malfunctioning equipment due to lack of maintenance.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 7m includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 7n.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 7o and 7p provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

### CIP-007-3a R3

RFC2016016341

ReliabilityFirst determined that the Entity did not evaluate a security patch for applicability within the appropriate timeframe as required by CIP-007-3a R3.

The cause of this violation was insufficient process. The Entity's patching process did not account for off-cycle or out of band patches.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS. Attachment 8a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its mitigation activities to address the referenced violation. A list of the mitigation activities is in the Settlement Agreement, included as Attachment 1.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 13

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachment 8b provides specific information on ReliabilityFirst's verification of the Entity's completion of the activities.

RFC2016016342

ReliabilityFirst determined that the Entity mistakenly believed that patches for certain programs were being tracked by a vendor when, in fact, they were not. Patches for certain programs were not tracked, evaluated, or installed.

The cause of this violation was insufficient workforce management leading to an incorrect assumption regarding the scope of vendor support.

ReliabilityFirst determined that this violation posed a serious risk to the reliability of the BPS. Attachment 8c includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 8d.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 8e and 8f provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

CIP-007-6 R2

RFC2016016343

ReliabilityFirst determined that the Entity was in violation of CIP-007-6 R2 in two instances. In the first instance, the Entity failed to take one of the following actions within 35 calendar days of completing a patch evaluation: (1) apply the patch; (2) create a dated mitigation plan; or (3) revise an existing mitigation plan. In the second instance, the Entity failed to install two [REDACTED] patches on five systems within the time provided by CIP-007-6 P 2.3.

The cause of this violation was insufficient procedures.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 14

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachments 9a and 9b include the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 9c.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 9d and 9e provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017017777

ReliabilityFirst determined that the Entity did not apply [REDACTED] software updates for [REDACTED] BES Cyber Assets ("BCAs").

The causes of this violation were a failure to follow an internal process and workforce management.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 9f includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 9g.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 9h and 9i provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017017839

ReliabilityFirst determined that several of the Entity's [REDACTED] group patches deployed to their [REDACTED] in the test environment were never deployed in the production environment.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 15

The cause of this violation was insufficient workforce management.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 9j includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan activities to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 9k.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 9l and 9m provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2018020386

ReliabilityFirst determined that the Entity installed [REDACTED] patches one day late and installed [REDACTED] patches 28 days late. Additionally, the patch evaluation for one patch cycle was completed one day late.

The cause of this violation was a deficient onboarding process.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 9n includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its mitigation activities to address the referenced violation. A list of the mitigation activities is in the Settlement Agreement, included as Attachment 1.

ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachment 9o provides specific information on ReliabilityFirst's verification of the Entity's completion of the activities.

CIP-007-6 R4

RFC2017017548

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 16

ReliabilityFirst determined that the Entity violated CIP-007-6 R4 in three instances. In the first instance, the Entity discovered that [REDACTED] BCAs managing the [REDACTED] environment were improperly configured. In the second instance, [REDACTED] identified [REDACTED] servers that were configured for local logging, but the logs were not being reviewed in accordance with CIP-007-6 P 4.4. In the third instance, [REDACTED] BCAs were not being monitored for security incidents.

The causes of this violation were insufficient asset and configuration management and insufficient process and workforce management.

ReliabilityFirst determined that this violation posed a serious risk to the reliability of the BPS. Attachment 10a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 10b.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 10c and 10d provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2018019469

ReliabilityFirst determined that the Entity violated CIP-007-6 R4 in two instances. In the first instance, the Entity was unaware that a system it relied upon to review logs, and to send security alerts if necessary, had not been receiving logs from an [REDACTED]. In the second instance, a [REDACTED] stopped communicating with the [REDACTED] tool. The disconnection triggered a [REDACTED] alert; however, the issue was not immediately brought to the attention of the appropriate subject matter expert ("SME"), which delayed follow-up work to understand and address the disconnection in a timely manner.

The cause of this violation was an insufficient process.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS. Attachment 10e includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.



NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 17

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 10f.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 10g and 10h provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2018020086

ReliabilityFirst determined that, in two instances, an asset was not sending logs to [REDACTED], which resulted in a failure to review logs and an inability to generate alerts for security events.

The cause of this violation was an insufficient process for asset identification and management.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS. Attachment 10i includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 10j.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 10k and 10l provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2019021564

ReliabilityFirst determined that the Entity was in violation of CIP-007-6 R4 in four instances. In three instances, the Entity experienced log collection and alerting issues affecting approximately [REDACTED] (43 percent) of its [REDACTED] assets. In the fourth instance, the Entity experienced log collection issues affecting [REDACTED] assets.

The cause of this violation was a lack of escalation and oversight in the [REDACTED] process.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 18

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS. Attachment 10m includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 10n.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 10o and 10p provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

CIP-007-6 R5

RFC2017016888

ReliabilityFirst determined that the Entity had four shared accounts on [REDACTED] [REDACTED] assets that did not meet the password complexity requirements in CIP-007-6 P5.5.

The causes of this violation were a deficient process and inadequate oversight.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 11a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 11b.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 11c and 11d provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

CIP-009-6 R1

RFC2016016384

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 19

ReliabilityFirst determined that the Entity was in violation of CIP-009-6 R1. The Entity implemented [REDACTED] firewalls [REDACTED]. The Entity had an overarching recovery plan that required the creation of certain recovery procedures; however, it did not have recovery procedures for the [REDACTED] firewalls.

The cause of this violation was insufficient asset and configuration management.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 12a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 12b.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 12c and 12d provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

#### CIP-010-2 R1

RFC2017017546

ReliabilityFirst determined that the Entity violated CIP-010-2 R1 in two instances. In the first instance, the Entity discovered that two PCAs were deployed to an Electric Security Perimeter ("ESP") even though the Entity did not have a documented baseline configuration as required by CIP-010-2 R1. In the second instance, the Entity replaced a server via its urgent change order process without getting the change order approved the day after the change due to a lack of a designated manager.

The cause of this violation was an insufficient process.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS. Attachment 13a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 20

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 13b.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 13c and 13d provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017017765

ReliabilityFirst determined that the Entity did not have a documented baseline configuration for two PCAs.

The cause of this violation was an insufficient process.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS. Attachment 13e includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 13f.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 13g and 13h provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017017840

ReliabilityFirst determined that the Entity's personnel were not documenting the results of required cyber security controls testing and verifications when performing non-routine configuration changes at the [REDACTED].

The cause of this violation was insufficient workforce management.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 13i includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 21

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 13j.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 13k and 13l provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017018307

ReliabilityFirst determined that the Entity inappropriately installed backup software on two PACS servers without proper authorization and testing.

The cause of this violation was insufficient workforce management.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 13m includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 13n.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 13o and 13p provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2018019647

ReliabilityFirst determined that the Entity did not have documented baselines for the existing [REDACTED] servers.

The causes of this violation were insufficient processes and procedures.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS. Attachment 13q includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 22

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 13r.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 13s and 13t provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

CIP-010-2 R3

RFC2017017836

ReliabilityFirst determined that, between July 2016 and March 2017, the Entity did not perform active vulnerability assessments of [REDACTED] assets prior to deploying said assets into a [REDACTED] production environment.

The cause of this violation was an insufficient procedure.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS. Attachment 14a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 14b.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 14c and 14d provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017018498

ReliabilityFirst determined that the Entity added assets to the production environment of [REDACTED] [REDACTED] prior to the performance of active vulnerability assessments.

The causes of this violation were insufficient processes and procedures.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 23

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 14e includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 14f.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 14g and 14h provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2018019048

ReliabilityFirst determined that the Entity did not complete a paper assessment or an active vulnerability assessment of [REDACTED] production assets within the 15 calendar month constraints of CIP-010-2 P3.1.

The causes of this violation were insufficient processes and workforce management.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 14i includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 14j.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 14k and 14l provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

CIP-010-2 R4

RFC2017018285

ReliabilityFirst determined that the Entity's personnel used an unauthorized laptop to connect to a switch.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 24

The cause of this violation was insufficient procedures.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 15a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 15b.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 15c and 15d provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

RFC2017018761

ReliabilityFirst determined that the Entity did not follow proper procedures for connecting a Transient Cyber Asset ("TCA") within a protected ESP.

The cause of this violation was inadequate training.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 15e includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 15f.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 15g and 15h provide specific information on the Entity's certification and ReliabilityFirst's verification of the Entity's completion of the activities, respectively.

CIP-011-2 R1

RFC2017017838



NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 25

ReliabilityFirst determined that the Entity did not identify or adequately protect BES Cyber System Information (“BCSI”) in [REDACTED] locations.

The cause of this violation was inadequate planning.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS. Attachment 16a includes the facts regarding the violation that ReliabilityFirst considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 16b.

The Entity certified that it had completed all mitigation activities. ReliabilityFirst verified that the Entity had completed all mitigation activities as of [REDACTED]. Attachments 16c and 16d provide specific information on the Entity’s certification and ReliabilityFirst’s verification of the Entity’s completion of the activities, respectively.

#### Regional Entity’s Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of four hundred fifty thousand dollars (\$450,000) for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors:

1. ReliabilityFirst considered RFC2017017304 as repeat noncompliance with CIP-006-6 R1, which served as an aggravating factor;<sup>5</sup>
2. The Entity admitted to, and accepted responsibility for, the violations, which ReliabilityFirst considered to be a mitigating factor in the penalty determination;
3. The Entity self-identified and self-reported most of the violations prior to a pending Compliance Audit;
4. The Entity was cooperative throughout the compliance enforcement process;

<sup>5</sup> ReliabilityFirst did not treat some of the Entity’s prior violations as aggravating compliance history, in part, because the time that has passed since the completion of mitigation for those violations supports the conclusion that processes and systems have evolved such that the current violations do not indicate a failure to mitigate the prior violations. Additionally, many of the current violations are more isolated in nature than the prior violations. Some of the prior violations involved different causes than the instant case, so the current violations do not represent recurring conduct warranting aggravation of the penalty. For the minimal risk violations that demonstrated the Entity’s ability to promptly identify and correct noncompliance, ReliabilityFirst did not consider the prior violations to be an aggravating factor. The Entity’s relevant prior noncompliance with CIP-006-6 R1 includes NERC Violation ID [REDACTED]

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 26

5. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. The violations RFC2017018708, RFC2017017778, RFC2017017568, RFC2017018261, RFC2017017152, RFC2017017547, RFC2017018166, RFC2017018857, RFC2016016343, RFC2017017777, RFC2017017839, RFC2018020386, RFC2017016888, RFC2016016384, RFC2017017840, RFC2017018307, RFC2017018498, RFC2018019048, RFC2017018285, RFC2017018761, and RFC2017017838 posed a minimal and not a serious or substantial risk to the reliability of the BPS;
7. The violations RFC2017018760, RFC2018019570, RFC2017017304, RFC2016016341, RFC2018019469, RFC2018020086, RFC2019021564, RFC2017017546, RFC2017017765, RFC2018019647, and RFC2017017836 posed a moderate and not a serious or substantial risk to the reliability of the BPS
8. The violations RFC2016016342 and RFC2017017548 posed a serious and substantial risk to the reliability of the BPS; and
9. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of four hundred fifty thousand dollars (\$450,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

### **Statement Describing the Assessed Penalty, Sanction, or Enforcement Action Imposed<sup>6</sup>**

#### **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,<sup>7</sup> the NERC BOTCC reviewed the violations on February 4, 2020 and approved the resolution between ReliabilityFirst and the Entity. In approving the resolution, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

<sup>6</sup> See 18 C.F.R. § 39.7(d)(4).

<sup>7</sup> N. Am. Elec. Reliability Corp., "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); N. Am. Elec. Reliability Corp., "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); N. Am. Elec. Reliability Corp., "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 27

In reaching this determination, the NERC BOTCC considered the factors listed above.

For the foregoing reasons, the NERC BOTCC approved the resolution and believes that the assessed penalty of four hundred fifty thousand dollars (\$450,000) 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**

For the reasons discussed below, NERC is requesting nonpublic treatment of certain portions of this filing pursuant to Sections 39.7(b)(4) and 388.113 of the Commission's regulations. This filing contains sensitive information regarding the manner in which the Entity has implemented controls to address security risks and comply with the CIP standards. As discussed below, this information, if released publicly, would jeopardize the security of the Bulk Power System and could be useful to a person planning an attack on Critical Electric Infrastructure. NERC respectfully requests that the Commission designate the redacted portions of the Notice of Penalty as non-public and as Critical Energy/Electric Infrastructure Information ("CEII"), consistent with Sections 39.7(b)(4) and 388.113, respectively.<sup>8</sup>

- a. The Redacted Portions of this Filing Should Be Treated as Nonpublic Under Section 39.7(b)(4) as They Contain Information that Would Jeopardize the Security of the Bulk Power System if Publicly Disclosed

Section 39.7(b)(4) of the Commission's regulations states:

The disposition of each violation or alleged violation that relates to a Cybersecurity Incident or that would jeopardize the security of the Bulk Power System if publicly disclosed shall be nonpublic unless the Commission directs otherwise.

Consistent with its past practice, NERC is redacting information from this Notice of Penalty according to Section 39.7(b)(4) because it contains information that would jeopardize the security of the BPS if publicly disclosed. NERC has previously filed dispositions of CIP violations on a nonpublic basis because

<sup>8</sup> 18 C.F.R. § 388.113(e)(1).

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 28

of this regulation.<sup>9</sup> Nonpublic treatment of redacted information, including the identity of the Entity and other details of the violations, depends on: 1) the nature of the CIP violations; 2) whether mitigation is complete; 3) the extent to which the disclosure of the Entity's identity would be useful to someone seeking to cause harm; 4) whether an audit has occurred since the violations; 5) whether the violations were administrative or technical in nature; and 6) the length of time that has elapsed since the filing of the Notice of Penalty.<sup>10</sup>

The redacted information in this Notice of Penalty includes details that could lead to identification of the Entity, and information about the security of the Entity's systems and operations, such as specific processes, configurations, or tools the Entity uses to manage their cyber systems. As the Commission has previously recognized, information related to CIP violations and cyber security issues, including the identity of the Entity, may jeopardize BPS security, asserting that "even publicly identifying which entity has a system vulnerable to a 'cyber attack' could jeopardize system security, allowing persons seeking to do harm to focus on a particular entity in the Bulk-Power System."<sup>11</sup>

Consistent with the Commission's statement, NERC is treating as nonpublic the identity of the Entity and any information that could lead to its identification.<sup>12</sup> Information that could lead to the identification of the Entity includes the Entity's name, its NERC Compliance Registry ID, and information regarding the size and characteristics of the Entity's operations.

NERC is also treating as nonpublic any information about the security of the Entity's systems and operations.<sup>13</sup> Details about the Entity's systems, including specific configurations or the tools/programs it uses to configure, secure, and manage changes to its BES Cyber Systems, would provide an adversary relevant information that could be used to perpetrate an attack on the Entity and similar entities that use the same systems, products, or vendors.

**b. The Redacted Portions of this Filing Should Also be Treated as CEII as the Information Could be Useful to a Person Planning an Attack on Critical Electric Infrastructure**

<sup>9</sup> In response to recent Freedom of Information Act requests, the Commission has directed public disclosure regarding the disposition of CIP violations. *See, e.g.*, Freedom of Information Act Appeal, FOIA No. FY18-75 (August 2, 2018); FOIA No. FY19-19 Determinations on Docket Nos. NP14-32 and NP14-41 (February 28, 2019). In those cases, the Commission directed public disclosure of the identity of the registered entity; the Commission did not disclose other details regarding the CIP violations.

<sup>10</sup> FOIA No. FY19-30, Second Notice of Intent to Release (June 13, 2019).

<sup>11</sup> *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards*, Order No. 672, 2006-2007 FERC Stats. & Regs., Regs. Preambles ¶ 31,204 at P 538 (Order No. 672).

<sup>12</sup> See the next section for a list of this information.

<sup>13</sup> See below for a list of this information.

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 29

In addition to the provisions of Section 39.7(b)(4), the redacted information also separately qualifies for treatment as CEII under Section 388.113 of the Commission's regulations. CEII is defined, in relevant part, as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that: (1) relates details about the production, generation, transmission, or distribution of energy; and (2) could be useful to a person planning an attack on critical infrastructure. As discussed above, this filing includes vulnerability and design information that could be useful to a person planning an attack on the Entity's critical infrastructure. The incapacity or destruction of the Entity's systems and assets would negatively affect national security, economic security, and public health and safety. For example, this Notice of Penalty includes the identification of specific cyber security issues and related vulnerabilities, as well as details concerning the types and configurations of the Entity's systems and assets. The information also describes strategies, techniques, technologies, and solutions used to resolve specific cyber security issues.

In addition to the name of the Entity, the following information has been redacted from this Notice of Penalty:

1. BES Cyber System Information, including security procedures; information related to BES Cyber Assets; individual IP addresses with context; group of IP addresses; Electronic Security Perimeter diagrams that include BES Cyber Asset names, BES Cyber System names, IP addresses, IP address ranges; security information regarding BES Cyber Assets, BES Cyber Systems, Physical Access Control Systems, Electronic Access Control and Monitoring Systems that is not publicly available; and network topology diagrams, etc.
2. The names of The Entity's vendors and contractors.
3. The NERC Compliance Registry number of the Entity.
4. The registered functions and registration dates of the Entity.
5. The names of the Entity's facilities.
6. The names of the Entity's assets.
7. The names of the Entity's employees.
8. The names of departments that are unique to the Entity.
9. The sizes and scopes of the Entity's operations.
10. The dates of Compliance Audits of the Entity, as those dates are included in schedules publicly posted by the Regional Entities.
11. The dates of Self-Reports submitted while preparing for Compliance Audits.
12. The Entity's compliance history.

Under Section 388.113, NERC requests that the CEII designation apply to the redacted information in Items 1-2 for five years from this filing date, April 30, 2020. Details about the Entity's operations,

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 30

networks, and security should be treated and evaluated separately from its identity to avoid unnecessary disclosure of CEII that could pose a risk to security. NERC requests that the CEII designation apply to the redacted information from Items 3-9 for three years from this filing date, April 30, 2020. NERC requests the CEII designation for three years to allow for several activities that should reduce the risk to the security of the BPS. Those activities include, among others:

1. Compliance monitoring of the Entity to ensure sustainability of the improvements described in this Notice of Penalty; and
2. Remediation of any subsequent violations discovered through compliance monitoring by ReliabilityFirst.

The Entity should be less vulnerable to attempted attacks following these activities. After three years, disclosure of the identity of the Entity may pose a lesser risk than it would today.

#### **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:

1. Settlement Agreement by and between ReliabilityFirst and the Entity executed [REDACTED], included as Attachment 1;
2. Record documents for the violation of CIP-002-5.1 R1 included as Attachment 2:
  - A. The Entity's Self-Report (RFC2017018708);
  - B. The Entity's Mitigation Plan designated as RFCMIT013479 submitted [REDACTED];
  - C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED]
3. Record documents for the violation of CIP-004-6 R2, included as Attachment 3:
  - A. The Entity's Self-Report (RFC2017017778);
  - B. The Entity's Mitigation Plan designated as RFCMIT012999 submitted [REDACTED];
  - C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED]
4. Record documents for the violations of CIP-004-6 R4, included as Attachment 4:
  - A. The Entity's Self-Report (RFC2017017568);
  - B. The Entity's Mitigation Plan designated as RFCMIT012980 submitted [REDACTED];

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 31

- C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - E. The Entity's Self-Report (RFC2017018261);
  - F. The Entity's Mitigation Plan designated as RFCMIT013213-1 submitted [REDACTED];
  - G. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - H. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - I. The Entity's Self-Report (RFC2017018760);
  - J. The Entity's Mitigation Plan designated as RFCMIT013443 submitted [REDACTED];
  - K. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - L. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
5. Record documents for the violation of CIP-004-6 R5, included as Attachment 5:
- A. The Entity's Self-Report (RFC2017017152) submitted [REDACTED];
  - B. The Entity's Self-Report (RFC2017017152) submitted [REDACTED];
  - C. The Entity's Mitigation Plan designated as RFCMIT012807-1 submitted [REDACTED];
  - D. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - E. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
6. Record documents for the violation of CIP-005-5 R2, included as Attachment 6:
- A. The Entity's Self-Report (RFC2018019570);
  - B. The Entity's Mitigation Plan designated as RFCMIT013868 submitted [REDACTED];
  - C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
7. Record documents for the violations of CIP-006-6 R1, included as Attachment 7:
- A. The Entity's Self-Report (RFC2017017304);
  - B. The Entity's Mitigation Plan designated as RFCMIT012854 submitted [REDACTED];
  - C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - E. The Entity's Self-Report (RFC2017017547);

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 32

- F. The Entity's Mitigation Plan designated as RFCMIT012890 submitted [REDACTED];
  - G. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - H. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - I. The Entity's Self-Report (RFC2017018166);
  - J. The Entity's Mitigation Plan designated as RFCMIT013214 submitted [REDACTED];
  - K. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - L. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - M. The Entity's Self-Report (RFC2017018857);
  - N. The Entity's Mitigation Plan designated as RFCMIT013482 submitted [REDACTED];
  - O. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - P. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
8. Record documents for the violations of CIP-007-3a R3, included as Attachment 8:
- A. The Entity's Self-Report (RFC2016016341);
  - B. ReliabilityFirst's Verification of Mitigating Activities Completion dated [REDACTED];
  - C. The Entity's Self-Report (RFC2016016342);
  - D. The Entity's Mitigation Plan designated as RFCMIT012397-1 submitted [REDACTED];
  - E. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - F. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
9. Record documents for the violations of CIP-007-6 R2, included as Attachment 9:
- A. The Entity's Self-Report (RFC2016016343), submitted [REDACTED];
  - B. The Entity's Self-Report (RFC2016016343) submitted [REDACTED];
  - C. The Entity's Mitigation Plan designated as RFCMIT012609 submitted [REDACTED];
  - D. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - E. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - F. The Entity's Self-Report (RFC2017017777);
  - G. The Entity's Mitigation Plan designated as RFCMIT013020 submitted [REDACTED];
  - H. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];



NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 33

- I. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - J. The Entity's Self-Report (RFC2017017839);
  - K. The Entity's Mitigation Plan designated as RFCMIT013016 submitted [REDACTED];
  - L. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - M. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - N. The Entity's Self-Report (RFC2018020386);
  - O. ReliabilityFirst's Verification of Mitigating Activities Completion dated [REDACTED];
10. Record documents for the violations of CIP-007-6 R4, included as Attachment 10:
- A. The Entity's Self-Report (RFC2017017548);
  - B. The Entity's Mitigation Plan designated as RFCMIT012983 submitted [REDACTED];
  - C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - E. The Entity's Self-Report (RFC2018019469);
  - F. The Entity's Mitigation Plan designated as RFCMIT013708 submitted [REDACTED];
  - G. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - H. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - I. The Entity's Self-Report (RFC2018020086);
  - J. The Entity's Mitigation Plan designated as RFCMIT014196 submitted [REDACTED];
  - K. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - L. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - M. The Entity's Self-Report (RFC2019021564);
  - N. The Entity's Mitigation Plan designated as RFCMIT014560 submitted [REDACTED];
  - O. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - P. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
11. Record documents for the violation of CIP-007-6 R5, included as Attachment 11:
- A. The Entity's Self-Report (RFC2017016888);
  - B. The Entity's Mitigation Plan designated as RFCMIT012746 submitted [REDACTED];

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 34

- C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
12. Record documents for the violation of CIP-009-6 R1, included as Attachment 12:
- A. The Entity's Self-Report (RFC2016016384);
  - B. The Entity's Mitigation Plan designated as RFCMIT012374 submitted [REDACTED];
  - C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
13. Record documents for the violations of CIP-010-2 R1, included as Attachment 13:
- A. The Entity's Self-Report (RFC2017017546);
  - B. The Entity's Mitigation Plan designated as RFCMIT012908 submitted [REDACTED];
  - C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - E. The Entity's Self-Report (RFC2017017765);
  - F. The Entity's Mitigation Plan designated as RFCMIT013013 submitted [REDACTED];
  - G. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - H. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - I. The Entity's Self-Report (RFC2017017840);
  - J. The Entity's Mitigation Plan designated as RFCMIT013022-1 submitted [REDACTED];
  - K. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - L. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - M. The Entity's Self-Report (RFC2017018307);
  - N. The Entity's Mitigation Plan designated as RFCMIT013267 submitted [REDACTED];
  - O. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - P. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - Q. The Entity's Self-Report (RFC2018019647);
  - R. The Entity's Mitigation Plan designated as RFCMIT013784-1 submitted [REDACTED];
  - S. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 35

- T. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
14. Record documents for the violations of CIP-010-2 R3, included as Attachment 14:
- A. The Entity's Self-Report (RFC2017017836);
  - B. The Entity's Mitigation Plan designated as RFCMIT013048 submitted [REDACTED];
  - C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - E. The Entity's Self-Report (RFC2017018498);
  - F. The Entity's Mitigation Plan designated as RFCMIT013394-1 submitted [REDACTED];
  - G. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - H. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - I. The Entity's Self-Report (RFC2018019048);
  - J. The Entity's Mitigation Plan designated as RFCMIT013546 submitted [REDACTED];
  - K. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - L. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
15. Record documents for the violations of CIP-010-2 R4, included as Attachment 15:
- A. The Entity's Self-Report (RFC2017018285);
  - B. The Entity's Mitigation Plan designated as RFCMIT013252 submitted [REDACTED];
  - C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
  - E. The Entity's Self-Report (RFC2017018761);
  - F. The Entity's Mitigation Plan designated as RFCMIT013445 submitted [REDACTED];
  - G. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
  - H. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
16. Record documents for the violation of CIP-011-2 R1, included as Attachment 16:
- A. The Entity's Self-Report (RFC2017017838);
  - B. The Entity's Mitigation Plan designated as RFCMIT013012 submitted [REDACTED];
  - C. The Entity's Certification of Mitigation Plan Completion dated [REDACTED];

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 36

D. ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 37

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

<p>*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.</p> <p>Robert V. Eckenrod* Vice President and General Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 Rob.Eckenrod@rfirst.org 216-503-0683 Phone</p> <p>Kristen M. Senk* Managing Enforcement Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 kristen.senk@rfirst.org 216-503-0669 Phone</p> <p>Thomas L. Scanlon* Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 tom.scanlon@rfirst.org 216-503-0658 Phone</p>	<p>Edwin G. Kichline* Senior Counsel North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net</p> <p>Alexander Kaplen* Associate Counsel North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile alexander.kaplen@nerc.net</p>
--	---

NERC Notice of Penalty  
The Entity  
April 30, 2020  
Page 38

### Conclusion

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

Respectfully submitted,

/s/ Alexander Kaplen

Edwin G. Kichline  
Senior Counsel  
Alexander Kaplen  
Associate Counsel  
North American Electric Reliability  
Corporation  
1325 G Street NW  
Suite 600  
Washington, DC 20005  
(202) 400-3000  
(202) 644-8099 - facsimile  
edwin.kichline@nerc.net  
alexander.kaplen@nerc.net

cc: The Entity  
ReliabilityFirst Corporation

Attachment 1

Settlement Agreement by and between ReliabilityFirst and  
the Entity executed [REDACTED]



# RELIABILITY FIRST

---

<i>In re:</i> [REDACTED]	)	<b>Violation ID Nos.:</b>
	)	
NERC Registry ID No. [REDACTED]	)	RFC2017018708 (CIP-002-5.1 R1)
	)	RFC2017017778 (CIP-004-6 R2)
	)	RFC2017017568 (CIP-004-6 R4)
	)	RFC2017018261 (CIP-004-6 R4)
	)	RFC2017018760 (CIP-004-6 R4)
	)	RFC2017017152 (CIP-004-6 R5)
	)	RFC2018019570 (CIP-005-5 R2)
	)	RFC2017017304 (CIP-006-6 R1)
	)	RFC2017017547 (CIP-006-6 R1)
	)	RFC2017018166 (CIP-006-6 R1)
	)	RFC2017018857 (CIP-006-6 R1)
	)	RFC2016016341 (CIP-007-3a R3)
	)	RFC2016016342 (CIP-007-3a R3)
	)	RFC2016016343 (CIP-007-6 R2)
	)	RFC2017017777 (CIP-007-6 R2)
	)	RFC2017017839 (CIP-007-6 R2)
	)	RFC2018020386 (CIP-007-6 R2)
	)	RFC2017017548 (CIP-007-6 R4)
	)	RFC2018019469 (CIP-007-6 R4)
	)	RFC2018020086 (CIP-007-6 R4)
	)	RFC2019021564 (CIP-007-6 R4)
	)	RFC2017016888 (CIP-007-6 R5)
	)	RFC2016016384 (CIP-009-6 R1)
	)	RFC2017017546 (CIP-010-2 R1 Part 1.1)
	)	RFC2017017765 (CIP-010-2 R1)
	)	RFC2017017840 (CIP-010-2 R1)
	)	RFC2017018307 (CIP-010-2 R1)
	)	RFC2018019647 (CIP-010-2 R1)
	)	RFC2017017836 (CIP-010-2 R3)
	)	RFC2017018498 (CIP-010-2 R3)
	)	RFC2018019048 (CIP-010-2 R3)
	)	RFC2017018285 (CIP-010-2 R4)
	)	RFC2017018761 (CIP-010-2 R4)
	)	RFC2017017838 (CIP-011-2 R1)

---



SETTLEMENT AGREEMENT  
BETWEEN  
RELIABILITYFIRST CORPORATION  
AND  
[REDACTED]

---

**I. INTRODUCTION**

1. ReliabilityFirst Corporation (“ReliabilityFirst”) and [REDACTED] (collectively, the “Parties”) enter into this Settlement Agreement (“Agreement”) to resolve violations by [REDACTED] of the above-captioned Reliability Standards and Requirements.<sup>1</sup>
2. The Parties stipulate to the facts in this Agreement for the sole purpose of resolving the violations. [REDACTED] admits that these facts constitute violations of the above-captioned Reliability Standards and Requirements and takes responsibility for the noncompliance.

**II. OVERVIEW** [REDACTED]

3. [REDACTED]
4. [REDACTED] is registered on the NERC Compliance Registry as a [REDACTED] in the ReliabilityFirst region. [REDACTED] in its capacity as a [REDACTED] is subject to compliance with the above-captioned Reliability Standard Requirements.

**III. EXECUTIVE SUMMARY**

*Brief Introduction*

5. This Agreement resolves 34 violations of Critical Infrastructure Protection (“CIP”)

---

<sup>1</sup> This Agreement references the version of the Reliability Standard in effect at the time each violation began. [REDACTED] however, committed to perform mitigating actions to comply with the most recent version of each Reliability Standard Requirement.

Reliability Standards and Requirements.<sup>2</sup> While the number of violations could appear to be excessive, the majority posed only minimal risk to the reliability of the Bulk Electric System (“BES”). And, this Agreement addresses, in substantial part, what ReliabilityFirst believes to be conduct reflective of continued and substantial improvements that [REDACTED] has made to its internal controls, compliance program, and culture.

6.

[REDACTED]

7.

[REDACTED]

*The* [REDACTED]

8.

[REDACTED]

9.

[REDACTED]

---

<sup>2</sup> The facts related to the violations are set forth in Attachment 1, which is incorporated herein by reference. Of the 34 total violations in this Agreement, ReliabilityFirst determined that 21 posed a minimal risk to the reliability of the BES, 11 posed a moderate risk to the reliability of the BES, and two posed a serious and substantial risk to the reliability of the BES.

<sup>3</sup>

[REDACTED]

[REDACTED]

10. In order to provide additional context for this Agreement, further explanation of

[REDACTED]

11. Here are some specific examples

[REDACTED]

12.

[REDACTED]

13.

[REDACTED]

*Overview of the Violations Resolved in This Agreement*

14. In advance of [REDACTED] ReliabilityFirst required and verified [REDACTED] mitigate the current violations as they were being submitted but, as described earlier, held many of the violations for processing so that it could fully understand and evaluate (a) the scope of the violations and (b) the results [REDACTED] security posture and implementing new tools, processes, and procedures.
15. The violations resolved in this Agreement do not involve and are not indicative of programmatic issues across [REDACTED] CIP compliance program. [REDACTED] identified many of the violations internally through controls that it has been implementing since [REDACTED] This Agreement resolves 36 Self-Reports [REDACTED] Importantly, a majority of [REDACTED] detailed minimal risk issues that were internally detected and short in duration.
16. ReliabilityFirst assigned 34 separate violation IDs to the 36 Self-Reports. Of the 34 total violations in this Agreement, ReliabilityFirst determined that 21 posed a minimal risk to the reliability of the BES, 11 posed a moderate risk to the reliability of the BES, and two posed a serious and substantial risk to the reliability of the BES.
17. Although the nature of the violations reflect a maturing compliance program, one violation of CIP-007-3a R3 (RFC2016016342) reflects a relatively significant oversight involving a failure to track, evaluate, and apply patches to several programs on [REDACTED]. The violation was discovered and remedied in [REDACTED], which demonstrates a dedication to self-identifying and correcting issues. Since the implementation of mitigating activities for the identified violation [REDACTED] has not experienced any patching violations relating to [REDACTED].
18. The other violation that posed a serious and substantial risk to the reliability of the BES involved multiple instances of noncompliance with CIP-007-6 R4 (RFC2017017548), including [REDACTED] failure to monitor certain assets, generate alerts for security events, and review logged security events. The number of devices that were affected coupled with the duration of the multiple instances increased the risk. Similar to the other serious and substantial risk violation, [REDACTED].

19. Some of the moderate risk violations involved issues encountered while implementing (or thereafter managing) new assets, technology, and infrastructure. For example, two moderate risk violations (RFC20170217546 and RFC2017017836) involved security and compliance issues that arose from shortcomings in ██████ asset deployment process, including insufficient guidance on the performance of specific tasks and a failure to delineate responsibilities. As another example, one moderate risk violation (RFC2019021564) involved ██████ management of technological and configuration errors during periodic outages of its ██████ that resulted in logging and alerting issues. Other moderate risk violations highlighted the need to continue training employees and evaluating and improving processes, procedures, and work instructions. For example, five moderate risk violations (RFC2016016341, RFC2017018760, RFC2018019469, RFC2017017765, and RFC2019019647) involved, to some degree, gaps in processes, procedures, or work instructions or personnel who did not fully understand their responsibilities.
20. ██████ remains dedicated to improving its processes, procedures, and work instructions and implementing new technology and infrastructure in an effort to develop and utilize industry best practices. As it continues developing and fine-tuning its infrastructure and program, it should encounter the types of issues described in the moderate risk violations less frequently, provided that it remains focused on fostering a culture of security, trains and supports personnel, and remains vigilant in developing and executing internal controls and preventing complacency.
21. Overall, the violations that are being resolved in this Agreement are mostly the result of a combination of contributing causes, including issues with implementing new assets, tools, and processes, inadequate training of staff, unclear or overlapping responsibilities, inadequate planning, and gaps in existing processes, procedures, and work instructions. Most of the violations were relatively short in duration. Regarding those with longer durations, ReliabilityFirst anticipates the less frequent occurrence of such problems as ██████ compliance program continues to mature.

*Overview of Penalty and Sanction*

22. Although ██████ has made significant improvements and the current violations are not indicative of programmatic issues, ReliabilityFirst determined that a penalty is appropriate in this case as a result of several moderate risk violations, some with relatively long durations, as well as the two serious risk violations. Accordingly, ReliabilityFirst has levied a monetary penalty of \$450,000.00.
23. It is worth noting that the issues for which ReliabilityFirst is imposing a sanction generally involved isolated issues, systems, assets, or assumptions or were related to (and began prior to) ██████ comprehensive improvement efforts. ReliabilityFirst believes ██████ has demonstrated a greatly-improved ability to promptly self-identify and correct issues and implores ██████ to continue its efforts and remain vigilant.

#### IV. ADJUSTMENT FACTORS

24. In addition to the facts and circumstances stated above, ReliabilityFirst considered the following factors in its penalty determination.

*Self-Identification and Voluntary Corrective Action*

25. Effective oversight of the reliability of the BES depends on robust and timely self-reporting by Registered Entities. [REDACTED] promptly identified and reported most of the violations at issue in this Agreement due to the effective execution of its compliance program and the installation of internal controls that yielded identification of the issues prior to the occurrence of any harm. Similarly, [REDACTED] voluntarily undertook corrective action. ReliabilityFirst seeks to encourage this type of detection, cessation, and reporting of offenses and, therefore, is applying mitigating credit relating to these violations.<sup>4</sup>

*Cooperation*

26. [REDACTED] has been highly cooperative throughout the entire enforcement process relating to these violations. Throughout the enforcement process, [REDACTED] voluntarily provided ReliabilityFirst with information that was timely, detailed, thoughtful, organized, and thorough. [REDACTED] fully cooperated in ReliabilityFirst's investigation of the violations and all associated mitigating activities and openly shared information regarding its processes, procedures, internal controls, assets, systems, and organization. This insight allowed ReliabilityFirst to better analyze the violations and assist [REDACTED] in resolving the same. Thus, ReliabilityFirst applied mitigating credit.

*Admission of Noncompliance*

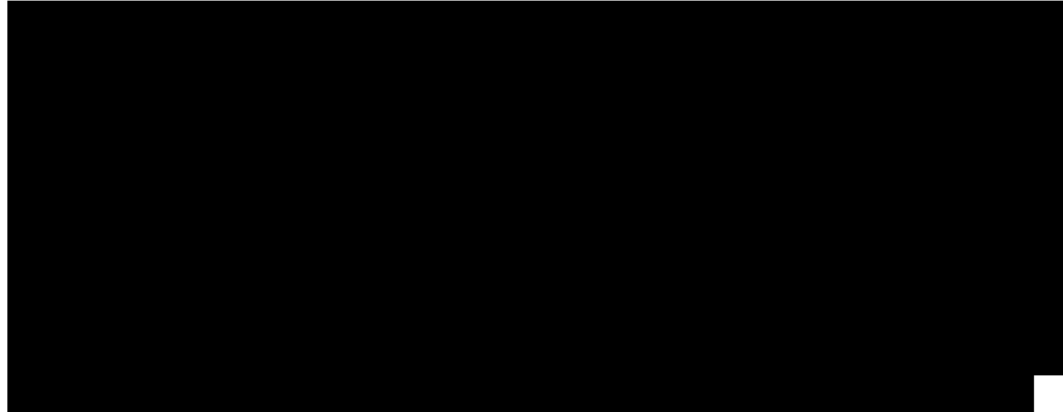
27. [REDACTED] recognized and affirmatively accepted responsibility for its conduct by admitting to the noncompliance resolved by this Agreement. ReliabilityFirst is applying mitigating credit since there is independent value in organizations accepting responsibility for their violations.

*Compliance History*

28. [REDACTED] has prior violations of [REDACTED]

---

<sup>4</sup> [REDACTED]



**V. PENALTY**

29. Based upon the foregoing, [REDACTED] shall pay a monetary penalty of \$450,000.00 to ReliabilityFirst.
30. ReliabilityFirst shall present an invoice to [REDACTED] within 20 days after the Agreement is approved by the Commission or affirmed by operation of law. Upon receipt, [REDACTED] shall have 30 days to remit payment. ReliabilityFirst will notify NERC if it does not timely receive the payment from [REDACTED]
31. If [REDACTED] fails to timely remit the monetary penalty payment to ReliabilityFirst, interest will commence to accrue on the outstanding balance, pursuant to 18 C.F.R. § 35.19a (a)(2)(iii), on the earlier of (a) the 31<sup>st</sup> day after the date on the invoice issued by ReliabilityFirst to [REDACTED] for the monetary penalty payment or (b) the 51<sup>st</sup> day after the Agreement is approved by the Commission or operation of law.

**VI. ADDITIONAL TERMS**

32. The Parties agree that this Agreement is in the best interest of BES reliability. The terms and conditions of the Agreement are consistent with the regulations and orders of the Commission and the NERC Rules of Procedure.
33. ReliabilityFirst shall report the terms of all settlements of compliance matters to NERC. NERC will review the Agreement for the purpose of evaluating its consistency with other settlements entered into for similar violations or under similar circumstances. Based on this review, NERC will either approve or reject this Agreement. If NERC rejects the Agreement, NERC will provide specific written reasons for such rejection and ReliabilityFirst will attempt to negotiate with [REDACTED] a revised settlement agreement that addresses NERC's concerns. If a settlement cannot be reached, the enforcement process will continue to conclusion. If NERC approves the Agreement, NERC will (a) report the approved settlement to the Commission for review and approval by order or operation of law and (b) publicly post the violations and the terms provided for in this Agreement.
34. This Agreement binds the Parties upon execution, and may only be altered or

NON-PUBLIC AND  
CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED  
FROM THIS PUBLIC VERSION

amended by written agreement executed by the Parties. [REDACTED] expressly waives its right to any hearing or appeal concerning any matter set forth herein, unless and only to the extent that [REDACTED] contends that any NERC or Commission action constitutes a material modification to this Agreement.

35. ReliabilityFirst reserves all rights to initiate enforcement action against [REDACTED] in accordance with the NERC Rules of Procedure in the event that [REDACTED] fails to comply with any of the terms or conditions of this Agreement. [REDACTED] retains all rights to defend against such action in accordance with the NERC Rules of Procedure.
36. [REDACTED] consents to ReliabilityFirst's future use of this Agreement for the purpose of assessing the factors within the NERC Sanction Guidelines and applicable Commission orders and policy statements, including, but not limited to, the factor evaluating [REDACTED] history of violations. Such use may be in any enforcement action or compliance proceeding undertaken by NERC or any Regional Entity or both, provided however that [REDACTED] does not consent to the use of the conclusions, determinations, and findings set forth in this Agreement as the sole basis for any other action or proceeding brought by NERC or any Regional Entity or both, nor does [REDACTED] consent to the use of this Agreement by any other party in any other action or proceeding.
37. [REDACTED] affirms that all of the matters set forth in this Agreement are true and correct to the best of its knowledge, information, and belief, and that it understands that ReliabilityFirst enters into this Agreement in express reliance on the representations contained herein, as well as any other representations or information provided by [REDACTED] to ReliabilityFirst during any [REDACTED] interaction with ReliabilityFirst relating to the subject matter of this Agreement.
38. Upon execution of this Agreement, the Parties stipulate that each possible violation addressed herein constitutes a violation. The Parties further stipulate that all required, applicable information listed in Section 5.3 of the CMEP is included within this Agreement.
39. Each of the undersigned agreeing to and accepting this Agreement warrants that he or she is an authorized representative of the party designated below, is authorized to bind such party, and accepts the Agreement on the party's behalf.
40. The undersigned agreeing to and accepting this Agreement warrant that they enter into this Agreement voluntarily and that, other than the recitations set forth herein, no tender, offer, or promise of any kind by any member, employee, officer, director, agent, or representative of the Parties has been made to induce the signatories or any other party to enter into this Agreement.
41. The Agreement may be signed in counterparts.
42. This Agreement is executed in duplicate, each of which so executed shall be deemed to be an original.



NON-PUBLIC AND  
CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED  
FROM THIS PUBLIC VERSION

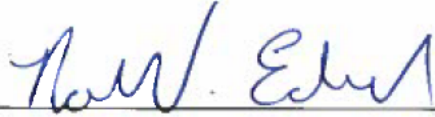
**[SIGNATURE PAGE TO FOLLOW]<sup>5</sup>**

**[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]**

---

<sup>5</sup> An electronic version of this executed document shall have the same force and effect as the original.

**ENDORSED BY:**



Robert Eckenrod  
Vice President and General Counsel  
ReliabilityFirst Corporation

OCT 14 2019

Date

**AGREED TO AND ACCEPTED BY:**



Date

**ReliabilityFirst Corporation**

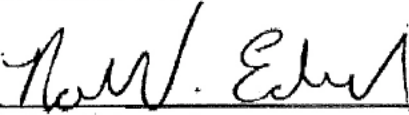


Timothy R. Gallagher  
President & Chief Executive Officer  
ReliabilityFirst Corporation

OCT 14 2019

Date

**ENDORSED BY:**

  
\_\_\_\_\_  
Robert Eckenrod  
Vice President and General Counsel  
ReliabilityFirst Corporation

OCT 14 2019  
\_\_\_\_\_  
Date

**AGREED TO AND ACCEPTED BY:**



**ReliabilityFirst Corporation**

  
\_\_\_\_\_  
Timothy R. Gallagher  
President & Chief Executive Officer  
ReliabilityFirst Corporation

OCT 14 2019  
\_\_\_\_\_  
Date

ATTACHMENT A

**VII. VIOLATIONS**

**A. CIP-002-5.1 R1 (RFC2017018708)**

43. CIP-002 ensures Bulk Electric System (“BES”) Cyber Systems and their associated BES Cyber Assets are identified to ensure protection against compromises that could lead to misoperation or instability in the BES.
44. A violation of CIP-002 R1 has the potential to affect the reliable operation of the bulk power system by providing the opportunity for exploitation of assets that are critical to the secure operation of the bulk power system.
45. CIP-002-5.1 R1 states, in part:
- R1.** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:
- i. Control Centers and backup Control Centers;
  - ii. Transmission stations and substations;
  - iii. Generation resources;
  - iv. Systems and facilities critical to system restoration, including Blackstart Resources and Crank Paths and initial switching requirements;
  - v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
  - vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

\*\*\*

- 1.2** Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

*Description of Violation and Risk Assessment for RFC2017018708*

46. On November 21, 2017, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-002-5.1 R1. *See*, Self-Report, **Attachment 1**. Specifically, [REDACTED] discovered that its [REDACTED] was incorrectly categorized as a [REDACTED] location. The [REDACTED] was controlling [REDACTED] and, therefore, should have been categorized as a [REDACTED] location. The issue was discovered during a design session for a [REDACTED].

47. The major contributing cause of the violation was a lack of sufficient controls to detect changes instituted in the control center. As new assets were integrated into the BES, [REDACTED] existing processes did not account for [REDACTED]. The major contributing cause implicates the management practice of asset and configuration management, which includes an entity's obligation to understand, account for, and control changes to its systems. It also implicates the management practice of implementation because when an entity decides to implement or modify assets, it is important to ensure that the new or modified assets do not compromise BES reliability and resilience.
48. The violation started on October 17, 2016, when [REDACTED]. Thereafter, [REDACTED] added [REDACTED].<sup>6</sup> The violation ended on November 14, 2017, when [REDACTED], thereby [REDACTED], which is [REDACTED].
49. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>7</sup> Incorrectly identifying and categorizing BES Cyber Systems and their associated BES Cyber Assets could result in compromise due to a corresponding failure to implement adequate and appropriate cyber security protections. Here, the risk was mitigated because although the [REDACTED] was incorrectly categorized, some security controls were in place and would have assisted in preventing compromise. For example: [REDACTED] assets were in a [REDACTED]. Further, [REDACTED] was not significant enough to increase the likelihood of an attack (i.e., it likely did not become a more attractive target for hostile actors as a result of [REDACTED]).
- Mitigating Actions for RFC2017018708*
50. On January 3, 2018, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-002-5.1 R1. See RFCMIT013479, **Attachment 2**. On January 29, 2018, ReliabilityFirst accepted the Mitigation Plan.
51. In the Mitigation Plan, [REDACTED] committed to take certain actions by April 9, 2018. First, [REDACTED] removed the [REDACTED] from the

<sup>6</sup> [REDACTED]

<sup>7</sup> CIP-002-5.1 R1 has a VRF of "High" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Lower" VSL.

Second, [REDACTED] modified its existing acquisition process(es) by adding a review/escalation process for all related business units for [REDACTED]. The process provided for escalation in the CIP-002 Program where necessary to address re-categorization evaluation. Third, [REDACTED] modified the CIP-002 Program to include a formal review of the change documentation from the modified acquisition process as well as [REDACTED] as part of the annual review.

52. On April 9, 2018, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of April 2, 2018. *See* Certification of Mitigation Plan Completion, **Attachment 3**. On August 27, 2018, ReliabilityFirst verified [REDACTED] completed the Mitigation Plan on March 19, 2018. *See*, Mitigation Plan Verification for RFCMIT013479, **Attachment 4**.

**B. CIP-004-6 R2 (RFC2017017778)**

53. CIP-004 increases the reliability of the Bulk-Power System by minimizing the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

54. A violation of CIP-004 R2 has the potential to affect the reliable operation of the BES by allowing individuals access to information without ensuring they are properly trained in how to use that information in a secure manner.

55. CIP-004-6 R2 states:

**R2.** Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2-Cyber Security Training Program.

**Part 2.2** Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.

*Description of Noncompliance and Risk Assessment for RFC2017017778*

56. On [REDACTED], [REDACTED] submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R2. *See* Self-Report, **Attachment 5**. During a scheduled [REDACTED] process, [REDACTED] discovered that an employee had physical access to a NERC asset prior to completing required training. Upon further investigation, [REDACTED] discovered that a programmer was tasked with updating [REDACTED]. [REDACTED] consisted of two [REDACTED] :

[REDACTED]. The programmer erroneously changed the definition of [REDACTED] to [REDACTED] or [REDACTED]. The incorrect logic allowed [REDACTED] personnel with either qualification to be granted [REDACTED]. Out of the [REDACTED] potential opportunities for access authorization errors, only one employee was granted access before completing required training. Said employee's manager requested the access through [REDACTED] and the access was granted because the incorrect [REDACTED] was in place for the employee.

57. The major contributing factor to this violation was inadequate training and instruction. [REDACTED] lacked a job aid defining the rules that make up a [REDACTED]. The major contributing factor implicates the management practice of workforce management, which includes the effective management and training of staff in support of their roles.
58. This violation started on April 12, 2017, when a [REDACTED] employee was granted unescorted physical access through [REDACTED] without having completed required training and ended on May 9, 2017, after [REDACTED] discovered and corrected the error.
59. ReliabilityFirst determined that the subject violation posed a minimal risk to the reliability of the BPS based on the following factors.<sup>8</sup> The violation has the potential to affect the reliable operation of the BES by providing an opportunity for unauthorized persons to access BES Cyber Systems and associated systems, potentially causing harm as a result of compromise or misuse. However, the risk was mitigated because the employee who obtained unauthorized access had a current personnel risk assessment ("PRA").<sup>9</sup> Moreover, the employee entered the Physical Security Perimeter ("PSP") for legitimate business reasons as evidenced by the fact that the employee's manager requested that access be granted through [REDACTED] thus further reducing the potential risk. Lastly, [REDACTED] internal processes quickly discovered the issue, and [REDACTED] resolved it in a timely manner.

*Mitigating Actions for RFC 2017017778*

60. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the subject violation with CIP-004-6 R2. See Mitigation Plan RFCMIT012999, **Attachment 6**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
61. In the Mitigation Plan, [REDACTED] committed to take the following actions by July 6, 2017. First, [REDACTED] revoked the [REDACTED] for the [REDACTED] employees who received it due to the coding error. Second, [REDACTED] created a process/job aid to provide instructions to qualification managers to ensure that changes/additions to qualifications satisfy requirements. An independent review was also implemented to serve as an additional control to ensure that changes to [REDACTED]

<sup>8</sup> CIP-004-6 R2 has a VRF of "Lower" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Lower" VSL.

<sup>9</sup> The additional [REDACTED] employees who could have had unauthorized access also had current PRAs.

are correct.

62. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of July 6, 2017. *See* Certification of Mitigation Plan Completion, **Attachment 7**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. *See*, Mitigation Plan Verification for RFCMIT012999, **Attachment 8**.

**C. CIP-004-6 R4 (RFC2017017568, RFC2017018261, and RFC2017018760)**

63. CIP-004 increases the reliability of the Bulk-Power System by minimizing the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

64. A violation of CIP-004 R4 has the potential to affect the reliable operation of the BES by providing the opportunity for unauthorized personnel at the Responsible Entity to access BES Cyber Systems and their associated Electronic Access Control and Monitoring and Physical Access Control Systems. Unauthorized access by unauthorized personnel could result in harm to the integrity of the BES Cyber Systems or the reliability of the BES as a result of intentional compromise or misuse.

65. CIP-004-6 R4 states:

**R4.** Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.

**Part 4.1** Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

**4.1.1.** Electronic access;

**4.1.2.** Unescorted physical access into a Physical Security Perimeter; and

**4.1.3.** Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

*Description of Violation and Risk Assessment for RFC2017017568*

66. [REDACTED], [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-004-6 R4. *See*, Self-Report, **Attachment 9**. [REDACTED] established a process for vendors to obtain remote access to



the [REDACTED]. On November 10, 2016, [REDACTED] employees did not follow that process. Specifically, an administrator responsible for access security assigned [REDACTED] to an employee in the [REDACTED] group without following the [REDACTED] process that required an approval from the [REDACTED] leader. Further, the administrator assigned the [REDACTED] in response [REDACTED]. The [REDACTED] employee provided the [REDACTED] to a vendor, thereby granting the vendor unauthorized remote access to the [REDACTED]. The unauthorized access was identified during the [REDACTED].

67. The major contributing factor to this violation was failure to follow established procedures and processes. This implicates the management practice of workforce management, which relates to the way an organization hires, manages, and trains staff.
68. The violation started on November 10, 2016, when [REDACTED] provisioned remote access to a vendor without following the process to authorize said access, and ended on May 3, 2017, when [REDACTED] revoked the [REDACTED].
69. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>10</sup> Providing unauthorized access to a network can be detrimental to the entity and the reliability of the BES as harm could be caused as a result of compromise or misuse. The risk was mitigated because [REDACTED] was provisioning access to the vendor for legitimate business purposes and simply failed to follow the proper procedure. Further [REDACTED] worked with the vendor frequently and retained [REDACTED] internally (i.e., the [REDACTED]; rather, [REDACTED]).

*Mitigating Actions for RFC2017017568*

70. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-004-6 R4. See RFCMIT012980, **Attachment 10**. [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
71. In the Mitigation Plan [REDACTED] committed to take certain actions by July 28, 2017. First [REDACTED] revoked access for [REDACTED]. Second, [REDACTED] took disciplinary action to correct the employee's behavior. Third, [REDACTED] updated the job aid to identify [REDACTED] when assigning to an owner. Fourth, [REDACTED] updated its procedures to indicate that a [REDACTED].

<sup>10</sup> CIP-004-6 R4 has a VRF of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Severe" VSL.

72. On [REDACTED] [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of July 28, 2017. See Certification of Mitigation Plan Completion, **Attachment 11**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. See Mitigation Plan Verification for RFCMIT012980, **Attachment 12**.

*Description of Violation and Risk Assessment for RFC2017018261*

73. On August 18, 2017, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED], it was in violation of CIP-004-6 R4. See, Self-Report, **Attachment 13**. On June 19, 2017, during a [REDACTED] training session, [REDACTED] discovered that [REDACTED] users had access to BES Cyber System Information (“BCSI”) without corresponding authorization records in [REDACTED]. Upon further investigation, [REDACTED] determined that [REDACTED] users maintained all qualifications required to have access to BCSI and that [REDACTED] users did not hold one or more of the proper qualifications. Specifically, [REDACTED] user who had administrator privileges to read, write, and delete BCSI did not maintain current NERC CIP training. And, [REDACTED] users who had privileges to read BCSI and write BCSI for their identified area did not have current NERC CIP training and valid PRAs.
74. The major contributing factor to this violation was a failure to implement sufficient controls, processes, and procedures. The procedure for bulk access provisioning did not include a requirement to verify the existence of authorization records in [REDACTED]. Such process and procedure gaps result in violations that are likely to be repeated. This implicates the management practice of verification. Before an entity implements a change or takes an action, it should verify (through established procedures and criteria) that the change or action is being made in accordance with requirements and will not adversely affect the BES.
75. The violation started on January 13, 2017, when [REDACTED] granted access to users who did not have corresponding authorization records and ended on August 4, 2017, when [REDACTED] completed the process of uploading corresponding authorization records and revoking access for those employees who did not have proper qualifications.
76. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>11</sup> Providing unauthorized or unqualified users access to BCSI increases the likelihood of misuse of that BCSI, thereby threatening the reliability of the BES. The risk was somewhat mitigated because all [REDACTED] users were trusted [REDACTED] personnel who were provisioned access for legitimate business reasons (i.e., maintenance of the system). Moreover, [REDACTED] users maintained proper qualifications to have access to BCSI but their records were not uploaded (i.e., for [REDACTED] users, this was simply a documentation issue). The issue was detected through internal controls, and no

---

<sup>11</sup> CIP-004-6 R4 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

harm is known to have occurred.

*Mitigating Actions for RFC2017018261*

77. On October 17, 2017, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-004-6 R4. See RFCMIT013213-1, **Attachment 14**. On October 23, 2017, ReliabilityFirst accepted the Mitigation Plan.
78. In the Mitigation Plan, [REDACTED] committed to take the following actions by August 30, 2017: first, [REDACTED] documented and updated its [REDACTED] bulk load process; second, [REDACTED] conducted a bulk upload for the [REDACTED] users into [REDACTED] and identified the users without proper access qualifications; third, [REDACTED] removed access for the [REDACTED] employees with missing qualifications; further, [REDACTED] revised its request for access [REDACTED] to include a requirement to verify that users are loaded into [REDACTED] prior to performing bulk access provisioning; and fifth, [REDACTED] conducted a [REDACTED] for the [REDACTED] employees with missing authorization records and removed any inappropriate access.
79. On October 27, 2017, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of August 4, 2017. See Certification of Mitigation Plan Completion, **Attachment 15**. On November 28, 2017, ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. See Mitigation Plan Verification for RFCMIT013213-1, **Attachment 16**.

*Description of Violation and Risk Assessment for RFC2017018760*

80. On December 1, 2017, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-004-6 R4. See, Self-Report, **Attachment 17**. During the [REDACTED], [REDACTED] identified [REDACTED] users who had access to a [REDACTED] that holds BCSI without corresponding authorization records in [REDACTED]. Further investigation showed that this exact same issue was identified during the [REDACTED]. After initially discovering the error during the [REDACTED], the users were marked for removal, and their supervisors requested revocations in [REDACTED]. Access for the [REDACTED] users was not revoked even though [REDACTED] indicated that the requests were completed and that access was revoked.
81. The major contributing factors to this violation were (a) ineffective controls, processes, and procedures, including a gap in the [REDACTED] as there was no requirement to verify evidence of access revocation prior to closing an [REDACTED], and (b) insufficient training. The [REDACTED] revocation of access tickets were closed prior to verifying that access was, in fact, revoked. This violation implicates the management practices of verification and workforce management. Verification was involved because there was a breakdown in the process of confirming that access had been revoked. Workforce management was involved because [REDACTED] staff should have been trained to verify that access was, in fact, revoked prior to closing the [REDACTED].

82. The violation started on April 1, 2017, when [REDACTED] failed to revoke access for [REDACTED] users and ended on November 29, 2017, when [REDACTED] actually completed the revocation process.
83. ReliabilityFirst determined that the violation posed a moderate risk to the reliability of the bulk power system based on the following factors.<sup>12</sup> Providing unauthorized access to a [REDACTED] that stores BCSI can be detrimental to the entity and the reliability of the BES as harm could be caused as a result of compromise or misuse. The risk was mitigated because all [REDACTED] users were trusted [REDACTED] personnel who had valid PRAs and up-to-date training records. Further, [REDACTED] had implemented effective internal controls which detected the issue, thereby further reducing the risk.

*Mitigating Actions for RFC20171018760*

84. On December 14, 2017, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-004-6 R4. *See RFCMIT013443, Attachment 18.* On January 4, 2018, ReliabilityFirst accepted the Mitigation Plan.
85. In the Mitigation Plan, [REDACTED] committed to take the following actions by January 10, 2018: first, [REDACTED] contacted the supervisors of all [REDACTED] users to revoke access to the [REDACTED] per the [REDACTED]; second, [REDACTED] reviewed and updated its [REDACTED] to include a requirement to verify the removal of access; and third [REDACTED] communicated the update to the team responsible for managing access authorizations.
86. On January 17, 2018, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of January 10, 2018. *See Certification of Mitigation Plan Completion, Attachment 19.* On March 12, 2018, ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. *See Mitigation Plan Verification for RFCMIT013443, Attachment 20.*

**D. CIP-004-6 R5 (RFC2017017152)**

87. CIP-004 increases the reliability of the Bulk-Power System by minimizing the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.
88. A violation of CIP-004 R5 has the potential to affect the reliable operation of the BES by allowing an individual to access BES Cyber Systems when that individual is no longer authorized to have such access.

---

<sup>12</sup> CIP-004-6 R4 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

89. CIP-004-6 R5 states:

**R5.** Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.

**Part 5.1** A process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights.)

\*\*\*

**Part 5.5** For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.

*Description of Violation and Risk Assessment for RFC2017017152*

90. On February 24, 2017 and March 1, 2017, [REDACTED] submitted Self-Reports to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-004-6 R5. *See*, Self-Reports, **Attachments 21** and **22**. This violation involved two separate instances.

91. Regarding the first instance, [REDACTED] did not initiate removal of the remote access capabilities of a security contractor’s employee within 24 hours of said person’s resignation on December 8, 2016. The employee of the security contractor worked at the [REDACTED] which is a [REDACTED]. Even though a supervisor deactivated the person’s physical access (i.e., identification badge), remote login capabilities were not deactivated. The remote access could have been used to access [REDACTED] system, which included access to [REDACTED]. The violation was discovered during the [REDACTED].

92. The major contributing factor to the first instance was insufficient training, as the supervisor knew to deactivate the identification badge but did not know to initiate removal of remote access. This implicates the management practice of workforce

management. Workforce management includes effective training to ensure personnel understand and follow processes and procedures.

93. Regarding the second instance, █████ failed to change a password for a shared account within 30 days after an employee who knew the password to the account voluntarily resigned. The shared account provided access to █████ which is an █████ server for █████ assets. The violation was discovered during an internal review.
94. The major contributing factor to the second instance was insufficient management and training, which implicates the management practice of workforce management. █████ maintained a procedure regarding password changes; however, responsible personnel were not aware of the procedure due to a breakdown in knowledge transfer as former responsible personnel transitioned to new roles. Workforce management includes promoting awareness and providing training to impart skills and knowledge to enable personnel to perform specific reliability and resilience functions.
95. The first instance started on December 9, 2016, when █████ failed to initiate removal of remote access capabilities and ended on January 10, 2017, when access was revoked. The second instance started on January 8, 2018, when █████ failed to change the password to the shared account and ended on January 30, 2018, when █████ changed the password.
96. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>13</sup> This violation has the potential to lead to misoperation or instability in the BES by allowing individuals to access BES Cyber Systems when said individuals should no longer have such access. However, the risk was mitigated by the following factors. Regarding both instances, the individuals voluntarily left the entity on good terms, thus reducing the likelihood that they would use remaining access in a way that would compromise the BES. Regarding the first instance, the potential risk was also reduced because the individual's physical access was promptly terminated, and the individual needed physical access to exploit the remaining cyber access. The entity verified, by reviewing access logs, that the individual did not use remote access capabilities after he left the entity. Regarding the second instance, although the password for the shared account had not been changed, █████ had removed all of the employee's electronic and physical access.

*Mitigating Actions for RFC2017017152*

97. On April 12, 2017, █████ submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-004-6 R5. See RFCMIT012807-1, **Attachment 23**. On April 12, 2017, ReliabilityFirst accepted the Mitigation Plan.

---

<sup>13</sup> CIP-004-6 R5 has a VRF of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Lower" VSL.

98. In the Mitigation Plan, [REDACTED] committed to take the following actions by May 23, 2017: first, [REDACTED] analyzed records to ensure that all security personnel with access privileges were still actively employed and had appropriate access; second, [REDACTED] revoked NERC access of the security contractor's employee who voluntarily resigned; third, [REDACTED] retrained leaders on the deactivation and revocation process; fourth, [REDACTED] updated the [REDACTED] shared account inventory to reflect the current shared account inventory; fifth, [REDACTED] developed a procedure with a checklist for transitioning SMEs between roles; sixth, [REDACTED] performed a quality check across all BES Cyber Assets ("BCAs") to see if there were other similar occurrences. As an additional mitigating activity relating to second instance described above, [REDACTED] changed the password for the shared account immediately after discovering the violation.
99. On May 30, 2017, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of May 18, 2017. *See Certification of Mitigation Plan Completion, Attachment 24.* On June 22, 2017, ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. *See Mitigation Plan Verification for RFCMIT012807-1, Attachment 25.*

**E. CIP-005-5 R2 (RFC2018019570)**

100. CIP-005 promotes the management of electronic access to Bulk Electric System ("BES") Cyber Systems by specifying a controlled Electronic Security Perimeter ("ESP") in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
101. A violation of CIP-005 R2 has the potential to affect the reliable operation of the BES by providing the opportunity for unauthorized access to an organization's network due to inadequate safeguards for remote access.
102. CIP-005-5 R2 states:
- R2.** Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2-Interactive Remote Access Management.
- Part 2.1** Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
- Part 2.2** For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.
- Part 2.3** Require multi-factor authentication for all Interactive Remote Access sessions.

*Description of Violation and Risk Assessment for RFC2018019570*

103. On April 11, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in noncompliance with CIP-005-5 R2. *See*, Self-Report, **Attachment 26**. In an effort to proactively assess its security posture, the entity hired a vendor to conduct a penetration test in late 2017. The vendor was retained, in part, to identify vulnerabilities and, in fact, identified the particular vulnerability that is the subject of this noncompliance. Specifically, [REDACTED] did not require multi-factor authentication to gain access to an ESP at a [REDACTED]. This individual could access [REDACTED] via single-factor authentication [REDACTED] and, thereby, gain access to an ESP.
104. The root causes of this noncompliance were inadequate planning and administrative oversight. The start date of this violation was the effective date of CIP-005-5 R2, and the entity lacked appropriate internal controls as evidenced by the fact that it did not identify this issue earlier (e.g., during v5/v6 implementation).
105. This noncompliance involves the management practice of asset and configuration management, which includes the need to maintain the integrity of assets and configuration items in order to increase reliability and resilience. It also involves the management practice of workforce management. Workforce management involves, in part, ensuring that personnel understand and implement appropriate security practices to promote reliability and resilience.
106. This noncompliance started on July 1, 2016, when the entity was required to implement multi-factor authentication for all Interactive Remote Access sessions but failed to do so in this particular instance and ended on December 5, 2017, when the entity corrected the issue.
107. This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors.<sup>14</sup> Single-factor authentication is less secure than multi-factor authentication. By allowing access without requiring multi-factor authentication, the entity increased the risk of compromise of the [REDACTED] and ESP. In this case, the risk was mitigated by the following facts. First, prior to accessing a specific asset within the ESP, an individual would need to know [REDACTED]. In other words, even if the [REDACTED] was compromised, a bad actor would have to further figure out [REDACTED] for assets within the ESP before the actor could cause any harm. Second, the entity otherwise complied with CIP-005-5 R2 (i.e., Intermediate Systems and encryption were utilized). It is also worth noting that the entity identified this particular issue by going above and beyond

---

<sup>14</sup> CIP-005-5 R2 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Moderate” VSL.



compliance with the reliability standards and retaining a vendor to conduct a thorough evaluation of the entity's security posture, and ReliabilityFirst seeks to encourage such endeavors. No harm is known to have occurred.

*Mitigating Actions for RFC2018019570*

108. On June 13, 2018, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the subject noncompliance with CIP-005-5 R2. See Mitigation Plan RFCMIT013868, **Attachment 27**. On July 12, 2018, ReliabilityFirst accepted the Mitigation Plan.
109. In the Mitigation Plan, [REDACTED] committed, in part, to take the following actions by August 15, 2018. The entity corrected the vulnerable configuration [REDACTED] immediately to avoid misuse of the vulnerable configuration. As an additional mitigating activity [REDACTED] verified that a similar condition did not exist on any other [REDACTED].
110. On August 15, 2018, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of August 3, 2018. See Certification of Mitigation Plan Completion, **Attachment 28**.<sup>15</sup> On February 7, 2019, ReliabilityFirst verified [REDACTED] completed the Mitigation Plan on August 3, 2018. See Mitigation Plan Verification for RFCMIT013868, **Attachment 29**.

**F. CIP-006-6 R1 (RFC2017017304, RFC2017017547, RFC2017018166, and RFC2017018857)**

111. CIP-006 ensures that a Responsible Entity manages physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber System against compromise that could lead to misoperation or instability in the BES.
112. A violation of CIP-006 R1 has the potential to affect the reliable operation of the BES by providing the opportunity to physically access Cyber Assets that are not protected by the implementation of a physical security plan.
113. CIP-006-6 R1 states:
  - R1.** Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1-Physical Security Plan.
    - Part 1.1** Define operational or procedural controls to restrict physical access.

---

<sup>15</sup> The certification indicates that the Mitigation Plan was completed on August 15, 2018, but the evidence submitted with the certification demonstrates that the Mitigation Plan was completed on August 3, 2018.

- Part 1.2** Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.
- Part 1.3** Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.
- Part 1.4** Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
- Part 1.5** Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan with 15 minutes of detection.
- Part 1.6** Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.
- Part 1.7** Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.
- Part 1.8** Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.
- Part 1.9** Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.
- Part 1.10** Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.

NON-PUBLIC AND  
CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED  
FROM THIS PUBLIC VERSION

Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:

- Encryption of data that transits such cabling and components; or
- Monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or
- An equally effective logical protection.

*Description of Violation and Risk Assessment for RFC2017017304*

114. On March 17, 2017 [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-006-6 R1. *See*, Self-Report, **Attachment 30**. The violation consists of three separate instances involving doors that were able to be opened regardless of an individual's previously assigned access privileges.
115. Regarding the first instance, on January 20, 2017, an employee who did not have authorized unescorted physical access swiped her badge at a [REDACTED] Physical Security Perimeter ("PSP") door (i.e., [REDACTED]). Both attempts generated an invalid attempt alarm followed by a forced door alarm, which alerted the [REDACTED] (" [REDACTED] "). The employee obtained access on the second attempt due to a door equipment failure.
116. The major contributing factor to the first instance was equipment malfunction. Security personnel investigating the incident were able to open PSP door [REDACTED] without swiping an access card.
117. In the second instance, on January 26, 2017, the door ajar alarm for a PSP door (i.e., [REDACTED]) was triggered. PSP door [REDACTED] [REDACTED]. During an investigation of the alarm, the doors appeared to be shut, but the alarm would not clear. Upon further investigation, it was discovered that the [REDACTED] which allowed to second door to intermittently remain ajar. After reviewing security camera footage, [REDACTED] discovered that six days earlier, on January 20, 2017, both sides of PSP door [REDACTED] were propped open to cool the room due to elevated equipment temperatures. [REDACTED] personnel followed internal protocol when the doors were propped open (i.e., notified security and implemented alternate security

measures while the doors were open). Upon completion of cooling, [REDACTED]  
[REDACTED]

118. The major contributing factor to the second instance was insufficient training and oversight. [REDACTED] personnel should have properly latched the second door, and their failure to do so rendered the PSP door unsecure.
119. Regarding the third instance, on January 28, 2017, a [REDACTED] employee called a [REDACTED] supervisor and reported that a PSP door (i.e., [REDACTED]) was malfunctioning. Specifically, individuals could pull the door open without swiping their badges. Security personnel investigated the matter and determined that the latch on the door was sticking, thereby preventing the door from remaining in the closed position.
120. The major contributing factor to the third instance was defective and malfunctioning equipment. The door and door hardware were not operating as intended.
121. This violation implicates the management practice of external interdependencies, which includes the need to monitor and manage the efforts of vendors whose services and products, such as doors and door hardware, may impact BES reliability and resilience. It also implicates the management practice of workforce management, which includes the need to train personnel and foster a culture of security.
122. The first instance started on January 20, 2017, when [REDACTED] employee gained access through a malfunctioning door and ended on the same day when [REDACTED] secured the door. The second instance started on January 26, 2017, when a PSP door became ajar and ended on the same day when [REDACTED] secured the door. The third instance began on January 28, 2017, when the door latch malfunctioned and ended on the same day when [REDACTED] called a vendor who completed repairs to the latch.
123. ReliabilityFirst determined that the violation posed a moderate risk to the reliability of the BPS based on the following factors.<sup>16</sup> [REDACTED] failure to control and restrict physical access could have permitted intruders to obtain access and inflict damage leading to instability in the BES. However, the risk was somewhat mitigated by the following factors. First, appropriate personnel at [REDACTED] were alerted of the issues in a timely manner. Said personnel responded, investigated, identified the causes of the issues, and remediated the issues. Second, additional security measures further reduced the risk (e.g., security perimeter fence and guard post, video surveillance, functioning alarms). Lastly, in the above-referenced instances, each individual who entered through the PSP doors did so for legitimate business reasons, thus further reducing the risk of harm.

---

<sup>16</sup> CIP-006-6 R1 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

*Mitigating Actions for RFC2017017304*

124. On May 1, 2017, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-006-6 R1. See RFCMIT012854, **Attachment 31**. On May 26, 2017, ReliabilityFirst accepted the Mitigation Plan.
125. In the Mitigation Plan, [REDACTED] committed to take certain actions by July 31, 2017. First, [REDACTED] conducted a study of the [REDACTED] PSP doors at the [REDACTED] including an inventory of all hardware, an examination of all maintenance performed, and a re-examination of [REDACTED]. Other industrial sites were benchmarked as part of the study to identify common equipment and human performance issues and resolutions. A two-phased approach was taken to implement PSP door security operations, maintenance, and testing: (1) phase one addressed the [REDACTED] most problematic doors; and (2) phase two addressed the remaining [REDACTED] doors. Second, [REDACTED] temporarily blocked off four doors that were identified as “high failure” during the aforementioned study. This was done in an effort to reduce recurrent alarm issues at these doors which consumed [REDACTED] resources. Third, [REDACTED] defined, documented, and communicated PSP Program roles and responsibilities to include [REDACTED]. Fourth, [REDACTED] developed a [REDACTED] to address business, functional, non-functional, and stakeholder requirements for PSP doors and door hardware located in industrial security environments. Fifth, [REDACTED] developed detailed pre-specifications for PSP single door and double door design types, which would address the doors and associated door hardware. Sixth, [REDACTED] developed and executed a [REDACTED] test plan for phase one PSP doors based on functional requirements and industrial design pre-specifications. The [REDACTED] included two standards: a [REDACTED] standard; and a [REDACTED] standard. Seventh, [REDACTED] tested one [REDACTED] and one [REDACTED]. The expected outcome for the tests was a ‘Go-No Go’ determination for implementing the [REDACTED] for the [REDACTED] most problematic doors and, thereafter, the [REDACTED] for the remaining [REDACTED] doors. Eighth, [REDACTED] implemented the [REDACTED]. Ninth, [REDACTED] implemented the [REDACTED].
126. On October 13, 2017, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of September 29, 2017.<sup>17</sup> See Certification of Mitigation Plan Completion, **Attachment 32**. On December 5, 2017, ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. See Mitigation Plan Verification for RFCMIT012854, **Attachment 33**.

---

<sup>17</sup> [REDACTED] was granted an extension of time to complete the Mitigation Plan.

*Description of Violation and Risk Assessment for RFC2017017547*

127. [REDACTED], [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-006-6 R1. *See*, Self-Report, **Attachment 34**. On March 16, 2017, contract security personnel conducted a monthly [REDACTED] at all [REDACTED] PSP doors. During testing, alarms were not triggered when a [REDACTED] PSP door in the [REDACTED] [REDACTED] was forced or propped open. The failures were documented on an inspection form, but the contract security personnel failed to create a maintenance ticket and activate and maintain alternate security measures until repairs and retesting were complete.<sup>18</sup> On April 10, 2017, [REDACTED] [REDACTED] personnel discovered the issue while conducting an internal audit. [REDACTED] implemented alternate security measures, created a maintenance ticket, and performed initial maintenance that same day. On April 11, 2017, a vendor was engaged to investigate the issue and repair and retest the alarms, which were experiencing issues due to improper wiring. Alternate security measures remained in place until April 21, 2017, at which point a follow-up review confirmed that the repairs fully resolved the issues.
128. The major contributing factor to this violation was faulty wiring. The issue persisted due to the fact that [REDACTED] contract security personnel failed to follow established processes and procedures. They discovered the issue during monthly testing; however, they failed to initiate required corrective action, thereby permitting the issue to continue until it was rediscovered during an internal audit and subsequently repaired.
129. This violation involves the management practice of external interdependencies, which includes the need to ensure that vendor's services and products are sufficient and operating properly for a secure environment.
130. The violation started on March 16, 2017, when the alarms malfunctioned and ended on April 11, 2017, when a vendor repaired the faulty wiring.
131. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>19</sup> Failing to maintain functioning alarms increases the likelihood that unauthorized access will not be detected, thereby increasing the risk of damage or instability in the BES due to compromise. Here, the risk was mitigated by the following factors. First, even though two of the alarms were not functioning properly, the door itself and additional security features (e.g., alarms monitoring for invalid access attempts and the badge card reader) were functioning properly, thus reducing the risk of compromise. Second, [REDACTED] utilizes a layered protection approach to physical security at the [REDACTED] which includes [REDACTED]

---

<sup>18</sup> The responsible contract security personnel were disciplined on April 17, 2017.

<sup>19</sup> CIP-006-6 R1 has a VRF of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Severe" VSL.

[REDACTED]. Lastly, the PSP door was approximately [REDACTED] feet from the [REDACTED] thus further reducing the risk of an intruder obtaining access without detection. It is also worth noting that [REDACTED] tests PSP doors monthly, meaning that issues are typically quickly discovered and addressed.

*Mitigating Actions for RFC2017017547*

132. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-006-6 R1. *See* RFCMIT012890, **Attachment 35**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
133. In the Mitigation Plan, [REDACTED] committed to take the following actions by May 8, 2017: first, [REDACTED] had a vendor inspect and repair the wiring; second, after the wiring was repaired, [REDACTED] validated that all alarm functionality was restored; third, [REDACTED] contract security vendor disciplined the two contract employees by removing one employee from [REDACTED] and removing one employee from duties at the [REDACTED] PSP; fourth, [REDACTED] provided alternate security measures at the door until the issue was fixed; fifth, [REDACTED] conducted a physical walk down of the [REDACTED] PSP to check for any signs of tampering within the PSP; sixth, [REDACTED] conducted a review of all [REDACTED] logs for the month of March, 2017, to ensure that no other barrier inspections contained failures that were not addressed; and seventh, [REDACTED] provided training to reinforce awareness of the maintenance and testing procedures to all staff responsible for maintenance and testing at [REDACTED] facilities.
134. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of May 8, 2017. *See* Certification of Mitigation Plan Completion, **Attachment 36**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. *See* Mitigation Plan Verification for RFCMIT012890, **Attachment 37**.

*Description of Violation and Risk Assessment for RFC2017018166*

135. On August 3, 2017, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-006-6 R1. *See*, Self-Report, **Attachment 38**.  
[REDACTED]  
[REDACTED] On May 25, 2017, [REDACTED] removed a [REDACTED] wall as part of a construction project, [REDACTED]  
[REDACTED] Restated, the exposed [REDACTED] was an unrestricted access point into a PSP (i.e., [REDACTED]) that

contained eight BES Cyber Assets.<sup>21</sup> The issue was discovered during a walk down on June 19, 2017.

136. The major contributing factor to this violation was insufficient planning and oversight of the construction project. [REDACTED] construction project management team did not evaluate whether the project would impact PSPs and, apparently, was not aware of the PSP protecting the [REDACTED].
137. This violation implicates the management practice of planning. Planning involves, in part, evaluating the potential impact of a project and identifying project risks. Inadequate planning can lead to unintended and undesirable consequences.
138. The violation started on May 25, 2017, when the [REDACTED] above the [REDACTED] was exposed, thereby providing an unrestricted access point into a PSP, and ended on June 20, 2017, when [REDACTED] blocked the access point.
139. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>22</sup> Failing to utilize physical access controls could result in an unauthorized person infiltrating a PSP and causing instability in the BES. Here, the risk was mitigated by the following facts. There are multiple layers of physical security at the [REDACTED]. Before a person could have [REDACTED] and accessed the [REDACTED], the person would have first been required to gain physical access to the [REDACTED] which is restricted and controlled by security. Further, the [REDACTED] was exposed in a room that was under construction, which obscured the opening, and there was no clear indication that the opening led to the [REDACTED], thus further reducing the risk. It is also worth noting that an after-the-fact investigation did not reveal evidence of tampering (e.g., [REDACTED] were in place and intact and items within the room were not moved or missing) or unauthorized access of software in the [REDACTED].

*Mitigating Actions for RFC2017018166*

140. On September 8, 2017, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-006-6 R1. See RFCMIT013214, **Attachment 39**. On October 4, 2017, ReliabilityFirst accepted the Mitigation Plan.
141. In the Mitigation Plan, [REDACTED] committed to take certain actions by November 17, 2017. First, [REDACTED] conducted a walk down the PSP to verify that no tampering of the cyber asset hardware occurred since the exposure on May 25, 2017. Second, [REDACTED] updated and disseminated its [REDACTED] procedures to address NERC CIP requirements for cyber assets to ensure that project managers are aware of, and account for, NERC CIP assets during project planning. Third,

---

<sup>21</sup> The BES Cyber Assets included [REDACTED].

<sup>22</sup> CIP-006-6 R1 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.



█ determined baselines and review █ logs to verify that no tampering of the cyber asset software occurred during the period of exposure. Fourth, █ updated project documents, including plans and schematics, to reflect the █ preventing █ access.

142. On November 17, 2017, █ certified to ReliabilityFirst that it completed this Mitigation Plan as of November 17, 2017. *See* Certification of Mitigation Plan Completion, **Attachment 40**. On November 28, 2017, ReliabilityFirst verified █ completion of this Mitigation Plan. *See* Mitigation Plan Verification for RFCMIT013214, **Attachment 41**.

*Description of Violation and Risk Assessment for RFC2017018857*

143. On December 14, 2017, █ submitted a Self-Report to ReliabilityFirst stating that, as a █ it was in violation of CIP-006-6 R1. *See*, Self-Report, **Attachment 42**. On November 28, 2017, a █ employee who had unescorted physical access privileges into a particular PSP at the █ entered said PSP through a locked door. Unbeknownst to the employee, the physical access control for the PSP was malfunctioning. The employee was carrying multiple cards with his █ access card and waved the cards in front of the badge reader for PSP Door █. The card reader denied access because it read the wrong card (i.e., the employee's gym access card). The employee did not realize that access was denied and was able to open the door despite being denied access. The █ was alerted of an invalid access attempt when the card reader denied access, and the forced entry alarm was triggered when the employee opened the door. Security personnel immediately responded to the alarms and investigated the issue.
144. The major contributing factor to this violation was malfunctioning equipment due to lack of maintenance. The locking mechanism on the door was malfunctioning, which allowed the door to be pulled opened even though the card reader denied access.
145. This violation implicates the management practice of grid maintenance, which includes the need to maintain equipment in a manner that is reliable and safe.
146. The violation started on November 28, 2017, when the locking mechanism malfunctioned and the employee entered the PSP and ended the same day when █ repaired the locking mechanism.
147. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>23</sup> Failing to control physical access could lead to an unauthorized person gaining access and engaging in conduct that could adversely affect the BES. Here, the risk was mitigated by the following factors. First, the alarm systems (i.e., invalid access attempt alarm and

---

<sup>23</sup> CIP-006-6 R1 has a VRF of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Severe" VSL.

forced entry alarm) were functioning, thereby increasing the likelihood of immediate detection of unauthorized entry and reducing the potential risk. Second, in this case, it was an authorized employee who entered the PSP for legitimate business reasons, which further reduced the risk.

*Mitigating Actions for RFC2017018857*

148. On January 8, 2018, █████ submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-006-6 R1. *See* RFCMIT013482, **Attachment 43**. On January 30, 2018, ReliabilityFirst accepted the Mitigation Plan.
149. In the Mitigation Plan, █████ committed to take the following actions by January 12, 2018. First, █████ reviewed alarm logs for forced-in and forced-out instances for all of the doors (█████) to ensure that a similar condition did not exist on any other door.<sup>24</sup> Second, █████ developed a █████ for maintenance of the doors. Third, █████ created a recurring Work Order (“WO”) in █████ for monthly maintenance of all PSP doors to ensure that a monthly WO is assigned and preventative maintenance is performed.
150. On January 31, 2018, █████ certified to ReliabilityFirst that it completed this Mitigation Plan. *See* Certification of Mitigation Plan Completion, **Attachment 44**. On March 10, 2018, ReliabilityFirst verified █████ completion of this Mitigation Plan as of January 9, 2018. *See* Mitigation Plan Verification for RFCMIT013482, **Attachment 45**.

**G. CIP-007-3a R3 (RFC2016016341 and RFC2016016342)**

151. CIP-007 ensures that Responsible Entities define methods, processes, and procedures for securing those systems determined to be CCAs as well as the non-CCAs within the ESP.
152. A violation of CIP-007 R3 has the potential to affect the reliable operation of the BES 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.
153. CIP-007 R3 states:
  - R3.** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

---

<sup>24</sup> This investigation revealed that the issue only existed at PSP Door █████

- 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.

*Description of Violation and Risk Assessment for RFC2016016341*

154. ██████████ submitted a Self-Report to ReliabilityFirst stating that, as a ██████████ it was in violation of CIP-007-3a R3.<sup>25</sup> See, Self-Report, **Attachment 46**. More specifically, ██████████ did not evaluate a security patch for applicability within the appropriate timeframe. The patch at issue was released by a vendor ██████████ on January 9, 2015, and it affected ██████████ ██████████ ██████████ ██████████ in the ██████████ environment. Several months later, on August 17, 2016, a SME installed the patch on the ██████████ but no formal evaluation of the patch was ever completed.
155. The major contributing factor to this violation was a deficient process. ██████████ patching process did not account for off-cycle or out of band patches.<sup>26</sup> The vendor (██████████) released the patch outside of its normal cycle. Due to ██████████ deficient process, ██████████ responsible personnel failed to check for the patch, never evaluated the patch, and, ultimately, installed the patch several months after its release.
156. This violation implicates the management practice of workforce management, which includes the responsibility to manage systems to minimize human factor issues. This can often be achieved by implementing thought-out, clear, and executable processes and procedures. Processes and procedures that fail to account for reasonably-expected events are unreliable and lead to an increase in human factor issues, such as forgetting to check for off-cycle patches.
157. The violation started on February 9, 2015, when ██████████ failed to evaluate the patch within the required time period and ended on August 17, 2016, after ██████████ corrected its deficient patch evaluation process and installed the patch.
158. ReliabilityFirst determined that the violation posed a moderate risk to the reliability of the bulk power system based on the following factors.<sup>27</sup> The failure to assess security patches could provide for the continued existence of known vulnerabilities, thereby providing bad actors additional time to exploit the vulnerabilities and adversely affect the BES. The length of this violation increased the risk, as ██████████ allowed the known vulnerabilities to exist for several months. However, the risk

---

<sup>25</sup> ██████████ initially submitted this matter as a violation of CIP-007-6 R2; however, after further investigation, ReliabilityFirst determined that it was a violation of CIP-007-3a R3.

<sup>26</sup> Off-cycle or out of band patches are patches that are released at some time other than the normal release time.

<sup>27</sup> CIP-007-3a R3 has a VRF of “Lower.” ReliabilityFirst determined that this violation warranted a “Severe” VSL.

was somewhat mitigated by the fact that, prior to exploiting the vulnerabilities, a bad actor would have first been required to be inside the network and have access to the affected [REDACTED]. No harm is known to have occurred.

*Mitigating Actions for RFC2016016341*

159. On [REDACTED], [REDACTED] submitted Mitigating Activities to ReliabilityFirst to address the issue with CIP-007-3a R3. For its mitigation, [REDACTED] committed to take the following actions by October 5, 2016. First, [REDACTED] evaluated all other patches released by [REDACTED] and the applicable patches were applied to the systems or included in a mitigation plan. Second, [REDACTED] updated the patching process to include off-cycle patching notifications. Third, [REDACTED] applied the patch at issue in this violation. Fourth, [REDACTED] conducted patching compliance [REDACTED] that included all employees involved in patching on or before October 5, 2016.
160. On [REDACTED], ReliabilityFirst verified that [REDACTED] completed these Mitigating Activities on October 5, 2016. See Mitigating Activities Verification for RFC2016016341, **Attachment 47**.

*Description of Violation and Risk Assessment for RFC2016016342*

161. [REDACTED], [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-007-3a R3.<sup>28</sup> See, Self-Report, **Attachment 48**. A vendor ([REDACTED] installed [REDACTED] workstations, and, thereafter, [REDACTED] installed several different programs on the workstations to support administrative work, including [REDACTED]. The programs were listed in the baseline; however, [REDACTED] mistakenly believed that patches for the programs were being tracked by [REDACTED] when, in fact, they were not. Restated, patches for the above-referenced programs were not tracked, evaluated, or installed. This issue was discovered on July 16, 2016 and affected approximately [REDACTED] workstations.
162. The major contributing factor to this violation was a false assumption by the [REDACTED] group regarding the scope of vendor support. The [REDACTED] group assumed that [REDACTED] was tracking patches for programs that had been installed on workstations when, in fact, [REDACTED] was not tracking said patches.
163. This violation implicates the management practice of external interdependencies. While it is necessary for entities to depend on outside organizations to provide certain goods and services, it is important to have processes in place to ensure that BES reliability and resilience are not negatively impacted. [REDACTED] needs to fully understand and evaluate its reliance on outside organizations and, if necessary, address any existing gaps.
164. The violation started on October 1, 2010, when [REDACTED] failed to identify patch sources

---

<sup>28</sup> [REDACTED] initially submitted this matter as a violation of CIP-007-6 R2; however, after further investigation, ReliabilityFirst determined that it was a violation of CIP-007-3a R3.

and track patches for several programs and ended on October 10, 2016, after [REDACTED] evaluated and applied patches.

165. ReliabilityFirst determined that the violation posed a serious and substantial risk to the reliability of the bulk power system based on the following factors.<sup>29</sup> The failure to track patches for installed programs (particularly programs that are commonly targeted by malware) on [REDACTED] workstations could lead to compromise of a vulnerable system, which could negatively affect the BES and result in a substantial loss of load. The length of this violation and the lack of awareness increased the risk. The risk was only somewhat mitigated by the following facts. First, there were very few vulnerabilities identified in the affected programs during the time of the violation. Additionally, [REDACTED] layered defenses further mitigated the risk. No harm is known to have occurred.

*Mitigating Actions for RFC2016016342*

166. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-007-3a R3. See RFCMIT012397-1, **Attachment 49**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
167. In the Mitigation Plan, [REDACTED] committed to take the following actions by July 31, 2017. First, [REDACTED] reviewed the patch source template and updated it show the correct patch source vendors. Second, [REDACTED] evaluated the newly identified patches from third party [REDACTED] sources for applicability. Third, [REDACTED] installed all applicable patches. Fourth, [REDACTED] held a meeting to review lessons learned among SMEs to share current practices related to determining software patch sources. Fifth, [REDACTED] conducted a group review of the taken mitigation activities. Sixth, [REDACTED] conducted an extent of condition and review current patch sources for all business units. Seventh, [REDACTED] split the [REDACTED] software packages, Operating Systems, and other packages and systems into two categories. Eighth, [REDACTED] verified that the remaining software was needed. Ninth, [REDACTED] removed unnecessary software. Tenth, [REDACTED] identified new patch sources and updated (or mitigated) as necessary software with a business reason that was not monitored by [REDACTED]
168. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of July 31, 2017. See Certification of Mitigation Plan Completion, **Attachment 50**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. See Mitigation Plan Verification for RFCMIT012397-1, **Attachment 51**.

**H. CIP-007-6 R2 (RFC2016016343, RFC2017017777, RFC2017017839, RFC2018020386)**

169. CIP-007 ensures that Responsible Entities select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against

---

<sup>29</sup> CIP-007-3a R3 has a VRF of “Lower.” ReliabilityFirst determined that this violation warranted a “Severe” VSL.

compromise that could lead to misoperation or instability in the BES.

170. A violation of CIP-007 R2 has the potential to affect the reliable operation of the BES by providing the opportunity for infiltration of unauthorized network traffic into the Electronic Security Perimeter (“ESP”) when security patches and upgrades are not installed on Cyber Assets within the ESP.

171. CIP-007-6 R2 states:

**R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2-Security Patch Management.

**Part 2.1** A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.

**Part 2.2** At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.

**Part 2.3** For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:

- Apply the applicable patches; or,
- Create a dated mitigation plan; or,
- Revise an existing mitigation plan.

Mitigation plans shall include the Responsible Entity’s planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.

**Part 2.4** For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.

*Description of Violation and Risk Assessment for RFC2016016343*

172. [REDACTED] and [REDACTED], [REDACTED] submitted Self-Reports to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-007-6 R2. See, Self-Reports, **Attachments 52 and 53.**

173. Regarding the first instance, a vendor (█████ issued a █████ patch report on July 1, 2016, which listed, in part, the following patch:  
█████  
█████ evaluated the patch and determined that it was applicable in a timely manner. However, █████ failed to take one of the following actions within 35 calendar days of completing the evaluation and determining that the patch was applicable: (1) apply the patch; (2) create a dated mitigation plan; or (3) revise an existing mitigation plan. █████ ultimately revised an existing mitigation plan<sup>30</sup> that addressed the vulnerabilities associated with the patch, but this task was not completed until 21 days after the deadline imposed by CIP-007-6 P 2.3.
174. The major contributing factor to the first instance was a deficient patching process. For example, █████ applicable █████ did not include a thorough checklist, and its patch evaluation and deployment template did not include a column regarding existing or new mitigation plans. Therefore, even though the patch was evaluated, responsible personnel failed to complete necessary follow-up actions in a timely manner (i.e., █████ failed to apply the patch, create a dated mitigation plan, or revise an existing mitigation plan). Such process and procedure gaps result in violations that are likely to be repeated. This implicates the management practice of workforce management, which includes the need to ensure personnel are aware of, and equipped to carry out, their responsibilities.
175. Regarding the second instance, █████ failed to install two █████ patches on five systems within the time provided by CIP-007-6 P 2.3. On July 1, 2016, a vendor (█████ issued a █████ patch report, which listed, in part, two █████ patches. The first patch related to a vulnerability that existed when a specially crafted █████ file was opened. Due to the vulnerability, an attacker could have taken control of the affected system and installed programs, viewed, changed, or deleted data, or created new accounts with full user rights. The second patch related to a vulnerability that existed in █████ which, if exploited, could have allowed an attacker to take control of an affected system. Workstations were primarily at risk due to this vulnerability. To exploit either vulnerability, user interaction was required (e.g., clicking a link or opening a file in an e-mail attack scenario or navigating to a compromised website in a web-browsing scenario). █████ evaluated both patches in a timely manner but failed to apply them within the 35-day window provided by CIP-007-6 P. 2.3. █████ identified the issue on October 5, 2016, and applied the patches the next day, which was 41 days after the deadline to apply the patches.
176. The major contributing factor to the second instance was also a deficient patching process. This issue related to five █████ in the █████ At the time of the second instance, the █████

---

<sup>30</sup> At the time the patch was released, █████ was utilizing multiple versions of █████ on various hardware and web servers, and █████ was aware of a number of █████ updates, which were listed in █████ patching spreadsheets. But, a █████ vendor █████ instructed █████ not to install newer versions of █████ due to a perceived adverse impact on another application.

had an individual who evaluated patches and a separate individual who applied patches specified in the evaluations. The evaluations were divided by operating system [REDACTED]

[REDACTED] This assisted the second individual in knowing which patches to apply. However, in the second instance, the patches did not apply to [REDACTED]. The individual completing the evaluation did not [REDACTED].

Thereafter, the evaluation sheet was informally left with the individual who was to apply the patches, and this person missed the two [REDACTED] patches due to a failure to recognize [REDACTED].

177. The second instance implicates the management practice of workforce management, which includes the need to strive for operational proficiency through well-defined and executable processes and procedures. Combining appropriately skilled staff with adequate processes, procedures, and work tools would minimize this type of violation.
178. The first instance started August 26, 2016, which was the date by which the patch should have been implemented or a mitigation plan should have been created or revised, and ended on September 23, 2016, when [REDACTED] revised the mitigation plan. The second instance started on August 26, 2016, which was the date by which the patches should have been implemented or a mitigation plan should have been created or revised, and ended on October 6, 2016, when the patches were applied.
179. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>31</sup> The failure to timely apply patches or ensure that an adequate plan is in place to mitigate the vulnerabilities addressed by said patches could lead to compromise of a vulnerable system, which could cause harm ranging from nuisance issues to a substantial loss of load. The risk was somewhat mitigated by the following facts. Regarding the first instance, an existing mitigation plan was in place which addressed the vulnerability of the security patch. The failure to update said mitigation plan was largely a documentation issue. Regarding the second instance, the five affected systems were otherwise up-to-date with patches, and use of the systems was restricted to authorized [REDACTED] personnel, thus further reducing the risk. Further, the five systems were not connected to the corporate network, so a user would not use the systems for e-mail or web access, which were the only attack vectors that could be used to exploit the existing vulnerabilities. It is also worth noting that both instances had a relatively short duration, and the second instance was resolved within 24 hours of its identification. No harm is known to have occurred.

---

<sup>31</sup> CIP-007-6 R2 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “High” VSL.



*Mitigating Actions for RFC2016016343*

180. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-007-6 R2. See RFCMIT012609, **Attachment 54**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
181. In the Mitigation Plan, [REDACTED] committed to take certain actions by February 17, 2017. First, [REDACTED] updated the existing mitigation plan to include the [REDACTED]. Second, [REDACTED] applied the missed patches to the [REDACTED]. Third, [REDACTED] created a new patch evaluation template. Fourth, [REDACTED] conducted a [REDACTED] of a formal handoff between evaluation and application of a patch via a pre-job brief. Fifth, [REDACTED] held a meeting to review lessons learned among representative SMEs to share current practices related to determining software patch sources. Sixth, [REDACTED] revised its [REDACTED] patch management process map to include the pre-job brief requirement. Seventh, [REDACTED] revised its patch mitigation plan template to include a section on revisions. Eighth, [REDACTED] revised its [REDACTED] to include the need for a task to be added to the change order when a mitigation plan needs to be created/revised. Ninth, [REDACTED] held a meeting among SMEs to share the changes to the mitigation plan and [REDACTED] process.
182. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan. See Certification of Mitigation Plan Completion, **Attachment 55**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan as of February 21, 2017. See Mitigation Plan Verification for RFCMIT012609, **Attachment 56**.

*Description of Violation and Risk Assessment for RFC2017017777*

183. [REDACTED], [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-007-6 R2. See, Self-Report, **Attachment 57**. During a BCA information validation activity at the [REDACTED] on May 8, 2017, a representative of [REDACTED] discovered that [REDACTED] software updates were not applied to [REDACTED] BCAs. The updates should have been installed by May 4, 2017. No plan was created or revised to mitigate the vulnerabilities addressed by the updates. [REDACTED] failure to apply the patches or create or revise a mitigation plan within 35 days of the patch evaluation was a violation of CIP-007-6 R2.3. A change order was initiated on May 24, 2017, to apply the patches, and the patch installation was completed the next day.
184. The major contributing factor to this violation was a failure to follow an internal process. Specifically, [REDACTED] patch application process includes a step [REDACTED] which requires an escalation if a scheduled patch deployment is not going to be completed in time. The escalation involves notifying a [REDACTED] representative, who will then create or revise a mitigation plan to address the issue. Here, the responsible SME was not going to, and in fact did not, apply the patch in

time but failed to initiate the escalation process which would have ensured compliance with CIP-007-6 P 2.3.

185. This violation implicates the management practice of workforce management. Workforce management was involved because [REDACTED] personnel should have been trained and better equipped to escalate the issue when it became clear that the patch was not going to be applied in time.
186. The violation started on May 5, 2017, after the deadline passed to either apply the software patches or create or revise a mitigation plan and ended on May 25, 2017, when [REDACTED] applied the software patches.
187. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>32</sup> Failing to update [REDACTED]. Here, the risk was somewhat mitigated because the prior version of the [REDACTED] continued to function. Moreover, the issue was quickly identified and resolved, thus further reducing the risk. No harm is known to have occurred.

*Mitigating Actions for RFC2017017777*

188. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-007-6 R2. See RFCMIT013020, **Attachment 58**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
189. In the Mitigation Plan, [REDACTED] committed to take the following actions by December 7, 2017: first, [REDACTED] deployed the [REDACTED] software updates to the [REDACTED] BCAs; second, [REDACTED] researched the workflow capabilities within [REDACTED] implementation to determine if a workflow could be created/configured to act as automated escalation and triggering controls within the patch management process; third, [REDACTED] developed a [REDACTED] patch deployment verification checklist; fourth, [REDACTED] tailored the existing [REDACTED] tool for the [REDACTED] use to generate a [REDACTED] from existing [REDACTED] baseline data; and fifth, [REDACTED] utilized the [REDACTED] feature of [REDACTED] for patch deployment verification.
190. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of December 1, 2017. See Certification of Mitigation Plan Completion, **Attachment 59**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. See Mitigation Plan Verification for RFCMIT013020, **Attachment 60**.

---

<sup>32</sup> CIP-007-6 R2 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Moderate” VSL.

*Description of Violation and Risk Assessment for RFC2017017839*

191. [REDACTED], [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-007-6 R2. *See*, Self-Report, **Attachment 61**. In May, 2017, [REDACTED] discovered that several [REDACTED] group patches deployed to their [REDACTED] in the test environment were never deployed in the production environment.<sup>33</sup> [REDACTED] relies on [REDACTED] as a patch source for its [REDACTED] and [REDACTED] distributes software updates as a package on the second Tuesday of every month. In February, 2017, [REDACTED] released patches (the “February Patches”), and [REDACTED] evaluated and approved the February Patches in March, 2017. However, after [REDACTED] evaluation, [REDACTED] withdrew its February Patches due to an error. [REDACTED] re-released the corrected February Patches as part of its March package (the “March Patches”), and [REDACTED] evaluated and approved the March Patches that same month. The March Patches were deployed to the [REDACTED] test environment in March, 2017, without any issue; however, [REDACTED] inadvertently applied the February Patches in the production environment. As a result of this error, several assets were not running with the latest version of [REDACTED] which is used to [REDACTED]. After discovery of the issue, the updates were applied on May 7, 2017.
192. The major contributing factors to this violation were [REDACTED] variation from its standard patch distribution process (i.e., releasing the February Patches, recalling the February Patches, and re-releasing corrected February Patches as part of the March Patches) coupled with [REDACTED] inadequate manual processes which increased the likelihood of error. This implicates the management practice of workforce management, which includes the need to effectively manage staff performance, in part, by implementing systems and procedures that minimize human factor issues.
193. The violation started on April 28, 2017, the date by which the entity was required to either apply the March Patches or create a mitigation plan, and ended on May 7, 2017, when [REDACTED] applied the March Patches.
194. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>34</sup> Failing to apply patches or create or revise a mitigation plan in a timely manner could lead to exploitation of a known vulnerability and a breakdown of system security, which could result in misoperation or instability in the BES. Here, the risk was somewhat mitigated. First, the affected [REDACTED] were originally assumed to be NERC assets; however, upon further evaluation, [REDACTED] determined that the assets did not meet the [REDACTED] and, consequently, decommissioned the [REDACTED] from the NERC asset list on May 31, 2017. Because the [REDACTED] were not, in fact, NERC assets, the overall threat to the BES from a potential compromise was reduced. Second, access to the

<sup>33</sup> The issue was discovered during a monthly [REDACTED] Quality Assessment of [REDACTED] evidence.

<sup>34</sup> CIP-007-6 R2 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Lower” VSL.

affected software was restricted to system administrators and intended users, thus further reducing the risk. Third, the affected assets were otherwise up-to-date, and all prior patches were maintained. Lastly, the issue was quickly identified and resolved.

*Mitigating Actions for RFC2017017839*

195. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-007-6 R2. *See* RFCMIT013016, **Attachment 62**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
196. In the Mitigation Plan, [REDACTED] committed to take the following actions by July 6, 2017. First, [REDACTED] utilized [REDACTED]. Second, [REDACTED] integrated all applicable Cyber Assets that are updateable and for which a patching source exists into the [REDACTED]. Third, [REDACTED] implemented an [REDACTED]. Fourth, [REDACTED] updated the patching process to include [REDACTED]. Fifth, [REDACTED] reconciled its CIP-002 list to ensure that [REDACTED] assets are in the [REDACTED].
197. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of July 6, 2017. *See* Certification of Mitigation Plan Completion, **Attachment 63**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. *See* Mitigation Plan Verification for RFCMIT013016, **Attachment 64**.

*Description of Violation and Risk Assessment for RFC2018020386*

198. On August 29, 2018, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-007-6 R2. *See*, Self-Report, **Attachment 65**. On April 21, 2018, a new SME started with [REDACTED] and was assigned CIP compliance activities for PACS. The former SME had an informal handoff to the new SME, which included training and allowing the new SME to shadow her during patch installations and related tasks in May, 2018. The patches evaluated in May should have been deployed on or before June 21, 2018. [REDACTED] patches were installed one day late, and [REDACTED] patches were installed 28 days late. In addition, the patch evaluation for the June patch cycle was completed one day late. After the initial Self-Report, the entity reported an additional instance during a subsequent patching cycle involving two patches that were applied twenty-three days late.
199. The major contributing factor to this violation was a deficient onboarding process. The knowledge transfer between the former SME and the new SME was ad hoc and unsuccessful and did not include sufficient documentation. The new PACS SME did not have sufficient training and guidance to successfully complete the

required tasks.<sup>35</sup> The additional instance was caused by technical issues and, similar to the initial instance, insufficient training and guidance.

200. This violation implicates the management practice of workforce management. Workforce management was involved because the new SME should have been trained and better equipped to complete the patching tasks.
201. The violation started on June 22, 2018, after the deadline passed to install the patches that were evaluated in May, 2018, and ended on July 20, 2018, after the remainder of the patches were installed. The additional instance started on August 14, 2018, when the entity failed to apply two patches and ended on September 6, 2018, when the patches were applied.
202. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>36</sup> Failing to install patches on PACS could lead to exploitation of a known vulnerability and a breakdown of system security. Here, the risk was mitigated by the following factors. First, the entity discovered the issue through detective controls and recurring compliance meetings and diligently monitored and worked to resolve the issue, thereby reducing the risk. Second, the application of layered security, [REDACTED] [REDACTED] served to further mitigate the risk. No harm is known to have occurred.

*Mitigating Actions for RFC2018020386*

203. On August 29, 2018, [REDACTED] submitted to ReliabilityFirst Mitigating Activities to address the violation of CIP-007-6 R2. ReliabilityFirst accepted the Mitigating Activities.
204. For its mitigation, [REDACTED] committed to take the following actions. First, [REDACTED] verified completion of the May, 2018, patch cycle. Second, [REDACTED] corrected the job aid associated with patching. Third, the new SME completed the entity's NERC onboarding process. Fourth, [REDACTED] published the formal NERC onboarding process, which will now be utilized for all incoming SMEs completing NERC-related tasks.
205. On April 2, 2019, ReliabilityFirst verified [REDACTED] completed these Mitigating Activities on August 24, 2018. See Mitigating Activities Verification for RFC2018020386, **Attachment 66**.

**I. CIP-007-6 R4 (RFC2017017548, RFC2018019469, RFC2018020086, and RFC2019021564)**

206. CIP-007 ensures that Responsible Entities define select technical, operational, and

---

<sup>35</sup> Technical issues encountered by the new SME resulted in some PACS instability; however, no failures of physical access controls were discovered.

<sup>36</sup> CIP-007-6 R2 has a VRF of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Moderate" VSL.

procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

207. A violation of CIP-007 R4 has the potential to affect the reliable operation of the BES by impeding a Registered Entity's ability to detect and investigate unauthorized access, reconnaissance, and other malicious activity on BES Cyber Systems.

208. CIP-007-6 R4 states:

**R4.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4-Security Event Monitoring.

**Part 4.1** Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

**4.1.1.** Detected successful login attempts;

**4.1.2.** Detected failed access attempts and failed login attempts;

**4.1.3.** Detected malicious code.

**Part 4.2** Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):

**4.2.1.** Detected malicious code from Part 4.1; and

**4.2.2.** Detected failure of Part 4.1 event logging.

**Part 4.3** Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.

**Part 4.4** Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.

*Description of Violation and Risk Assessment for RFC2017017548*

209. On [REDACTED], [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a

██████████ it was in violation of CIP-007-6 R4. See, Self-Report, **Attachment 67**. This violation involves three separate instances.

210. Regarding the first instance, after ██████████ performed by ██████████ between January and March, 2017, ██████████ learned that ██████████ environment were improperly configured. This resulted in violations of CIP-007-6 R4.2 (i.e., failure to generate alerts for security events) and CIP-007-6 R4.3 (i.e., failure to retain event logs).
211. The major contributing factors to the first instance were (a) the use of incorrect protocols and (b) a misconfiguration of firewalls. Another contributing factor was ██████████ that used different asset naming conventions, which created a situation where asset IDs were mismatched during configuration. The first instance implicates asset and configuration management, which includes the need to effectively inventory, monitor, manage, and control assets and configuration items. It also implicates the management practice of validation because ██████████ failed to test and confirm that intended results were achieved (i.e., that ██████████ were properly configured to generate alerts and that event logs were, in fact, being retained).
212. In the second instance, ██████████ identified ██████████ that were configured for local logging, but the logs were not being reviewed in accordance with CIP-007-6 P 4.4. The second instance was also discovered after the ██████████ performed by ██████████ between January and March, 2017.
213. The major contributing factors to the second instance were a deficient monitoring process and a lack of communication. Specifically, as part of its administration of its ██████████ monitoring process, ██████████ did not provide business units with adequate insight into monitoring activities that were being performed, which created a scenario where the business unit responsible for reviewing the local logs incorrectly assumed that the logs were being reviewed by a separate business unit. The second instance implicates the management practice of workforce management, which includes the obligation to minimize human factor issues through effective communication, training, and procedures.
214. The third instance involved ██████████ assets (BCAs) at the ██████████ that were not being monitored for security incidents. In July, 2016, a senior engineer with the ██████████ sent ██████████ for assets that needed to be monitored to the ██████████ team. On December 22, 2016, the ██████████ inquired as to the status of their assets being logged and monitored by the ██████████ group. The ██████████ group informed the ██████████ that there was no log for the above-referenced ██████████ assets. Further investigation revealed that a vendor ██████████ disabled logging for the assets in order to execute troubleshooting and never reactivated it.

215. The major contributing factors to the third instance were (a) a vendor disabling logging for the affected assets and (b) [REDACTED] lack of awareness of the vendor's activities. This implicates the management practice of external interdependencies, which includes the need to ensure that a vendor's products and services are not negatively impacting security and BES reliability and resilience.
216. The first instance started on July 1, 2016, when [REDACTED] failed to configure [REDACTED] to generate security alerts and ended on March 13, 2017, after [REDACTED] corrected the errors and configured the assets to send alerts. The second instance started on July 1, 2016, when [REDACTED] failed to review logs for the [REDACTED] and ended on March 17, 2017, when [REDACTED] decommissioned the [REDACTED]. The third instance started on July 1, 2016, when [REDACTED] failed to monitor, or generate security alerts for, [REDACTED] assets and ended on January 25, 2017, when the issue was corrected.
217. ReliabilityFirst determined that the violation posed a serious and substantial risk to the reliability of the bulk power system based on the following factors.<sup>37</sup> Failing to monitor assets and send alerts for security incidents significantly impairs an entity's ability to maintain real-time situational awareness and investigate cyber security events. The number of devices that were affected coupled with the duration of time of this violation significantly increased the risk of exploitation or a cyber-related attack. Further, [REDACTED] displayed a lack of effective project management controls, including a failure to verify that its processes were actually working and a failure to ensure that a vendor completed its work in an acceptable manner.

*Mitigating Actions for RFC2017017548*

218. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-007-6 R4. See RFCMIT012983, **Attachment 68**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
219. In the Mitigation Plan, [REDACTED] committed to take the following actions by July 12, 2017. First, [REDACTED] corrected all [REDACTED]. Second, [REDACTED] established a clear location for storing collected logs. Third, [REDACTED] generated failed login attempts to confirm that relevant logs and alerts were indeed generated and sent to the appropriate contacts. Fourth, [REDACTED] updated the [REDACTED] and [REDACTED] procedure to state that all [REDACTED] of the NERC Assets need to be sent out to [REDACTED] personnel to verify that they receive [REDACTED] from the [REDACTED]. Fifth, [REDACTED] updated its [REDACTED] to include responsibilities for [REDACTED] SMEs to review for accuracy and completeness of [REDACTED] monitored assets every quarter. Sixth, [REDACTED] reviewed assets sending events to [REDACTED] and matched that with the BES Cyber Systems list. Seventh, [REDACTED] enhanced its [REDACTED] process to define a process for verifying logging configurations after

---

<sup>37</sup> CIP-007-6 R4 has a VRF of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Severe" VSL.



implementation to confirm intended outcomes are achieved.

220. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of July 12, 2017. *See* Certification of Mitigation Plan Completion, **Attachment 69**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. *See* Mitigation Plan Verification for RFCMIT012983, **Attachment 70**.

*Description of Violation and Risk Assessment for RFC2018019469*

221. On March 26, 2018, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-007-6 R4. *See*, Self-Report, **Attachment 71**. This violation involves two separate instances.
222. Regarding the first instance, [REDACTED] was unaware that a system it relied upon to review logs, and to send security alerts if necessary, had not been receiving logs from an [REDACTED]. The issue was discovered by the [REDACTED] administrator during an ad hoc review of the [REDACTED] [REDACTED] which displayed that the asset was no longer communicating with the [REDACTED].
223. The major contributing factor to the first instance was a configuration error. On December 19, 2017, [REDACTED] implemented a change to an antivirus client. Due to a configuration error relating to the change, the [REDACTED] was disconnected from the [REDACTED] and an alert was not generated to notify appropriate personnel of a failure of event logging.<sup>38</sup> The first instance implicates the management practice of validation, which includes the need to have checks in place to confirm that changes to systems meet their intended purpose and do not create or introduce new vulnerabilities.
224. In the second instance, [REDACTED] discovered that on September 15, 2017, a [REDACTED] stopped communicating with the [REDACTED]. The disconnection triggered a [REDACTED] however, the issue was not immediately brought to the attention of the appropriate SME, which delayed follow-up work to understand and address the disconnection in a timely manner.<sup>39</sup>
225. The major contributing factor to the second instance was a deficient process. [REDACTED] [REDACTED] stopped communicating with the [REDACTED] however, there was a lack of a formal process regarding next steps. There should have been troubleshooting and an escalation step in the monitoring and response process, which would have increased the likelihood of the issue being addressed in a timely manner. Instead, the asset remained disconnected. This instance involves the management practice of

<sup>38</sup> [REDACTED] was manually configuring each connected asset, and the [REDACTED] was missed, resulting in the disconnection.

<sup>39</sup> [REDACTED] uses [REDACTED] to [REDACTED].

validation, which includes the need to ensure that a process functions as it is expected to in its environment and, if it does not, to fix the process.

226. The first instance started on December 19, 2017, when the [REDACTED] was disconnected from the [REDACTED] and no alert was generated and ended on February 16, 2018, when the connection was restored. The second instance started on September 15, 2017, when the [REDACTED] stopped communicating with the [REDACTED] and ended on March 30, 2018, when the connection was restored.
227. ReliabilityFirst determined that the violation posed a moderate risk to the reliability of the bulk power system based on the following factors.<sup>40</sup> Failing to properly log security events, generate alerts, and review logs increases the risk of undetected compromise of a BCA, potentially leading to misoperation or instability in the BES. The risk was somewhat mitigated by the following facts. The affected assets were located within a PSP, and cyber controls such as antivirus monitoring and change management were in place. It is also worth noting that [REDACTED] reviewed the available local logs for both assets, and there were no alerts that required further investigation.<sup>41</sup>

*Mitigating Actions for RFC2018019469*

228. On April 9, 2018, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-007-6 R4. *See* RFCMIT013708, **Attachment 72**. On May 4, 2018, ReliabilityFirst accepted the Mitigation Plan.
229. In the Mitigation Plan, [REDACTED] committed to take certain actions by May 2, 2018. First, [REDACTED] modified and published a test template [REDACTED]. Second, [REDACTED] conducted an extent of condition review to ensure that these two assets were the only assets not being appropriately monitored.<sup>42</sup> Third, [REDACTED] reconnected the assets to [REDACTED] to ensure that the two assets that stopped sending logs to [REDACTED] server started sending logs again. Fourth, [REDACTED] ensured that the assets maintained logs locally at the time of the disconnections. Fifth, [REDACTED] reviewed logs stored locally to ensure that the two assets local logs did not contain alerts/alarms that required attention. Sixth, [REDACTED] modified its [REDACTED] to ensure that a process was in place to prevent mishandling of [REDACTED] offensives. Seventh, [REDACTED] modified the frequency of [REDACTED] reports to ensure all assets have been reviewed for

---

<sup>40</sup> CIP-007-6 R4 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “High” VSL.

<sup>41</sup> Logs were collected locally for the [REDACTED] involved in these instances, but the logs were not forwarded or reviewed. An after-the-fact investigation revealed that only the last 90 days of logs could be reviewed since older local logs were automatically purged from the workstations.

<sup>42</sup> Although no additional instances were found through this extent of condition review, the review was later determined to be insufficient. The review was manual and required [REDACTED] personnel to examine and reconcile extensive sets of documents. Flaws in the review process were ultimately exposed when [REDACTED] discovered additional instances that should have been identified earlier as part of the review (i.e., the instances described in RFC2018020086).

completeness to prevent prolonged disconnections. Eighth, [REDACTED] formalized the ad hoc review cadence to ensure all assets had been reviewed for completeness to prevent prolonged disconnections.

230. On May 2, 2018, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of May 2, 2018. *See* Certification of Mitigation Plan Completion, **Attachment 73**. On July 5, 2018, ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. *See* Mitigation Plan Verification for RFCMIT013708, **Attachment 74**.

*Description of Violation and Risk Assessment for RFC2018020086*

231. On July 17, 2018, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-007-6 R4. *See*, Self-Report, **Attachment 75**. Specifically, [REDACTED] discovered that an [REDACTED] [REDACTED] was not sending logs to [REDACTED] which resulted in a failure to review logs and an inability to generate alerts for security events. An old certificate file (2008) was installed and configured on the asset, which prevented logs from being sent to [REDACTED] for monitoring and alerting. The issue was identified on June 14, 2018, when a SME was reviewing a monthly report and discovered that [REDACTED] was not monitoring the [REDACTED].
232. During the process of mitigating the above-referenced violation, [REDACTED] discovered an additional instance.<sup>43</sup> Specifically, another [REDACTED] asset was not properly configured to send logs to the [REDACTED] and, therefore, no alerts were being generated for security events. However, logs were being stored locally.
233. The major contributing factor to these violations was a deficient process for asset identification and management. [REDACTED] [REDACTED] did not include any detailed steps instructing SMEs to verify that assets were, in fact, sending logs to the [REDACTED] [REDACTED]. This violation implicates the management practice of asset and configuration management, which includes the need to properly inventory, monitor, manage, and control assets and configuration items. It also implicates the management practices of verification and validation.
234. [REDACTED] [REDACTED] administrators could not determine if [REDACTED] had ever received logs for the asset referenced in the first instance, and, therefore, the start date for this violation was the implementation date for CIP-007-6 R4, which was July 1, 2016. The first instance ended on June 25, 2018, when [REDACTED] updated the certificate file and connected the asset to [REDACTED]. The start date for the additional instance was March 22, 2018, which is the date that the asset was placed into production. The additional instance ended January 16, 2019, when the asset was properly configured

---

<sup>43</sup> Similar to the previous violation, an extent of condition review did not reveal this additional instance. Again, the review was later determined to be insufficient because it was manual and required [REDACTED] personnel to examine and reconcile extensive sets of documents. As described in the mitigation section for this violation, [REDACTED] ultimately improved the review process to reduce the likelihood of recurrence.

to send logs to the [REDACTED]

235. ReliabilityFirst determined that the violation posed a moderate risk to the reliability of the bulk power system based on the following factors.<sup>44</sup> Failing to monitor assets and generate alerts for security events creates a significant gap that a wrongdoer could exploit and leverage to attack the entity and BES. Such an attack likely would have been undetected. The length of time of this violation increased the risk. Moreover, [REDACTED] missed a number of opportunities to identify and manage the affected assets for security events. In the first instance, the asset should have been identified during the CIP v5/v6 transition. Further, [REDACTED] missed opportunities for identification during cyber vulnerability assessments. In both instances, [REDACTED] failed to discover the issues during previous extent of condition reviews for separate instances. The risk was somewhat mitigated by the fact that the assets were [REDACTED]

*Mitigating Actions for RFC2018020086*

236. On October 12, 2018, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the subject noncompliance with CIP-007-6 R4. See Mitigation Plan RFCMIT014196, **Attachment 76**. On October 16, 2018, ReliabilityFirst accepted the Mitigation Plan.
237. In the Mitigation Plan, [REDACTED] committed to take the following actions by December 21, 2018. First, [REDACTED] ensured that the [REDACTED] had the correct certificate file installed and would begin to be monitored by [REDACTED]. Second, as part of its [REDACTED] [REDACTED] had SMEs review assets and confirm and attest that each asset that is capable of sending logs was configured correctly and, in fact, sending logs to [REDACTED]. Third, [REDACTED] conducted an [REDACTED] to identify the root cause of the violation and address countermeasures. Fourth, [REDACTED] updated its asset management process to include instructions for SMEs to verify that assets were logging correctly and connected to [REDACTED]. Fifth, [REDACTED] communicated the updated process to SMEs.
238. Further, after identifying the additional instance referenced in this violation, [REDACTED] developed and implemented [REDACTED] November, 2018, that will assist with verifying that all applicable [REDACTED] assets were connected to the [REDACTED]
239. On December 19, 2018, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan. See Certification of Mitigation Plan Completion, **Attachment 77**. On February 15, 2019, ReliabilityFirst verified [REDACTED] completed the Mitigation Plan on December 17, 2018. See Mitigation Plan Verification for RFCMIT014196, **Attachment 78**.

---

<sup>44</sup> CIP-007-6 R4 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “High” VSL.

*Description of Noncompliance and Risk Assessment for RFC2019021564*

240. On May 14, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R4. See Self-Report, **Attachment 79**. To perform cyber security monitoring, the entity utilizes a [REDACTED] that consists, in part, of [REDACTED]. This noncompliance involves four primary, separate instances when the entity experienced technical issues and instability in its [REDACTED] that resulted in a loss of log collection and alerting functionality for certain [REDACTED] assets.
241. During the first instance (i.e., December 27, 2018, through January 15, 2019), the entity experienced log collection and alerting issues affecting approximately [REDACTED] (or 43%) of its [REDACTED] assets. Throughout the duration of the first instance, the entity worked with two vendors who support vital components of the [REDACTED] (i.e., [REDACTED]) to identify and resolve the issues. On January 11, 2019, the entity and vendors identified a [REDACTED] in the [REDACTED] (and ruled out the [REDACTED] components) as the root cause of ongoing issues. On January 15, 2019, the entity reestablished connectivity, and logging and alerting resumed.
242. During the second instance (i.e., February 13, 2019, through March 1, 2019), the [REDACTED] components went down. After the entity corrected the [REDACTED] issue and reestablished connectivity on January 15, 2019, the entity began experiencing intermittent issues with the [REDACTED] components, and overall [REDACTED] performance appeared to be degrading. The entity opened a ticket with [REDACTED] and worked diligently between January 16, 2019, and February 12, 2019, to identify and resolve any issues, but the [REDACTED] components stopped working on February 13, 2019. This resulted in log collection and alerting issues affecting approximately [REDACTED] (or 43%) of the entity's [REDACTED] assets. The entity immediately opened a critical ticket with [REDACTED]. Between February 13, 2019, and February 27, 2019, the entity worked diligently to resolve the issue, including several rounds of troubleshooting, escalating the issue with [REDACTED] to ensure adequate vendor support, and installing [REDACTED] developed custom fixes. The issue was resolved on February 27, 2019, but on February 28, 2019, the entity experienced connectivity issues due to [REDACTED].
243. The third instance was more isolated and discrete in nature. During the third instance (i.e., March 1, 2019, through March 29, 2019), the entity was more closely monitoring its [REDACTED] architecture to confirm that it had been successfully stabilized. The entity discovered that five assets were not sending logs to the [REDACTED]. On March 27, 2019, the entity determined that the issue was due to [REDACTED], and on March 29, 2019, the entity [REDACTED], thereby resolving the issue.

244. During the fourth instance (i.e., April 11, 2019, through April 23, 2019), the entity experienced another connection issue affecting approximately [REDACTED] (or 43%) of its [REDACTED] assets. Through investigation, the entity determined that a [REDACTED] was inadvertently configured to [REDACTED] on April 11, 2019. After discovery, the entity corrected the issue and restored the connection.
245. Collectively, the above-referenced circumstances resulted in multiple violations of CIP-007-6 R 4.1 (a failure to log events), CIP-007-6 R 4.2 (a failure to generate alerts for security events), CIP-007-6 R 4.3 (a failure to retain event logs), and CIP-007-6 R 4.4 (a failure to review a summarization or sampling of logged events). After the first instance, the entity was able to recover [REDACTED] of the missing data, and after the second instance, the entity was able to recover [REDACTED] of the missing data. A review of the recovered information yielded no evidence of malicious activity. The remainder of the data was lost for a variety of reasons, including [REDACTED]. Alerts for security events were not generated during any of the instances, and the entity also did not complete reviews in accordance with the mandates of CIP-007-6 R 4.4.
246. Technical issues, including a [REDACTED], were a contributing factor to these violations. However, the root cause of these violations was a lack of escalation and oversight in the [REDACTED] process. When the entity was working to recover [REDACTED] infrastructure and functionality, it should have alerted business units and asset owners of the infrastructure issues so that local logging tasks could be performed.
247. This noncompliance implicates the management practice of risk management. The purpose of risk management is to identify and evaluate potential problems before they occur so that an organization can plan for the potential problem and invoke appropriate risk mitigating activities when the problem is actually encountered. In this case, it was reasonably foreseeable that the technology relied upon as part of the entity's [REDACTED] could fail, and the entity should have planned for this potential problem and invoked appropriate risk mitigating activities when they actually encountered it.
248. The first instance started on December 27, 2018, when the entity began experiencing log collection and alerting issues due to a [REDACTED] in the [REDACTED] and ended on January 15, 2019, after the entity corrected the issue. The second instance started on February 13, 2019, when the entity began experiencing log collection and alerting issues due to a problem with [REDACTED] components and ended on March 1, 2019, after the problem was fully resolved. The third instance started on March 1, 2019, when five assets stopped logging [REDACTED] and ended on March 29, 2019, when the entity increased the [REDACTED]. The fourth instance started on April 11, 2019, when the [REDACTED] and ended on April 23, 2019, when the entity corrected the issue.

249. This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS based on the following factors.<sup>45</sup> Failing to log events, generate alerts, retain logs, and review a sample of logged events could impede an entity's ability to detect and investigate unauthorized access, reconnaissance, and other malicious activity on BES Cyber Systems. The risk was not serious and substantial in this case because the affected assets were afforded various cyber protections, including [REDACTED]. Even though the [REDACTED] (e.g., logging and alerting) was nonfunctional, security policies (e.g., [REDACTED]) were in place and would have helped to protect the assets. However, the risk was not minimal in this case because of the scope of the noncompliance (i.e., the number of affected [REDACTED]) and the entity's failure to consider and implement alternative measures when its technology (i.e., the [REDACTED]) failed. No harm is known to have occurred.

*Mitigating Actions for RFC2019021564*

250. On May 24, 2019, the entity submitted to ReliabilityFirst a Mitigation Plan to address the subject noncompliance with CIP-007-6 R4. *See* Mitigation Plan RFCMIT014560, **Attachment 80**. On May 28, 2019, ReliabilityFirst accepted the Mitigation Plan.
251. In the Mitigation Plan, the entity committed to take the following actions by August 15, 2019.<sup>46</sup> First, the entity updated its system monitoring process. The update included: (a) escalation steps to initiate manual log reviews and more timely data preservation; (b) test of alerts; and (c) enhanced monitoring of logging infrastructure. Second, the entity reviewed and updated the recovery procedure to promote quicker recovery in the future. Third, the entity created a checklist including standard functional configuration. Fourth, the entity performed a required read of the updated process.
252. On August 15, 2019, the entity certified to ReliabilityFirst that it completed this Mitigation Plan. *See* Certification of Mitigation Plan Completion, **Attachment 81**. On October 2, 2019, ReliabilityFirst verified [REDACTED] completed the Mitigation Plan on August 3, 2019. *See* Mitigation Plan Verification for RFCMIT014560, **Attachment 82**.

**J. CIP-007-6 R5 (RFC2017016888)**

253. CIP-007 ensures that Responsible Entities define select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

---

<sup>45</sup> CIP-007-6 R4 has a VRF of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Severe" VSL.

<sup>46</sup> The entity requested, and was granted, an extension of time to complete the referenced Mitigation Plan.

254. A violation of CIP-007 R5 has the potential to affect the reliable operation of the BES by allowing an unauthorized individual to access a facility using a default account.
255. CIP-007-6 R5 states:
- R5.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5-System Access Controls.

**Part 5.5** For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:

- 5.5.1.** Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and
- 5.5.2.** Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.

*Description of Violation and Risk Assessment*

256. On January 23, 2017, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-007-6 R5. *See, Self-Report, Attachment 83.* [REDACTED] identified four shared accounts on [REDACTED] assets at the [REDACTED] that did not meet the password complexity requirements set forth in CIP-007-6 P 5.5. A total of [REDACTED] users had access to the shared accounts.<sup>47</sup> The issue was initially discovered during an internal Annual Vulnerability Assessment on March 1, 2016, which was prior to the effective date of the above-referenced standard and requirement. However, the local [REDACTED] vulnerability management process was not followed, which allowed the issue to persist. The issue was re-discovered during a monthly internal audit of [REDACTED] BCAs in November, 2016, because the random audit sample included the affected assets.
257. The major contributing factors to this violation were (a) a deficient process and (b) inadequate oversight. The issue was identified, and should have been addressed, prior to the effective date of CIP-007-6; however, responsible personnel did not follow the vulnerability management process, which was unclear and did not include escalations. As a result, the issue persisted until it was re-discovered and, ultimately, corrected. This violation implicates the management practice of

---

<sup>47</sup> [REDACTED] had previously completed background checks of all [REDACTED] users who had access to shared accounts for the assets, and each user had completed required NERC training.



workforce management. Workforce management was involved because [REDACTED] personnel should have been trained and better equipped to resolve the issue in a timely manner, and the applicable process should have been clearer and included escalations.

258. The violation started on July 1, 2016, when [REDACTED] failed to utilize passwords that met the complexity requirements set forth in CIP-007-6 and ended on December 3, 2016, when the passwords were changed.
259. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>48</sup> Weak passwords increase the risk of successful password cracking attacks, which could lead to compromise of BES Cyber Systems and misoperation or instability in the BES. The risk was mitigated by the following facts. The assets were [REDACTED]. Further, the passwords were custom (i.e., not manufacturer defaults). The issue was quickly resolved after it was re-discovered, and it is worth noting that the re-discovery of this issue demonstrates the effectiveness of [REDACTED] internal review procedures.

#### *Mitigating Actions*

260. On March 20, 2017, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-007-6 R5. See RFCMIT012746, **Attachment 84**. On April 13, 2017, ReliabilityFirst accepted the Mitigation Plan.
261. In the Mitigation Plan, [REDACTED] committed to take the following actions by May 12, 2017. First, [REDACTED] conducted a [REDACTED] Annual Vulnerability Assessment. Second, [REDACTED] received an Annual Vulnerability Risk Assessment from [REDACTED]. Third, [REDACTED] brought shared account passwords for the [REDACTED] assets into compliance with password length and complexity requirements. Fourth, [REDACTED] identified all assets containing shared accounts at the [REDACTED] and verify they met NERC CIP-007-6 Part 5.5 standards for password length and complexity requirements. Fifth, [REDACTED] updated the [REDACTED] vulnerability management process document to clarify [REDACTED]. Sixth, [REDACTED] updated [REDACTED] to include a note that shared accounts must meet NERC-CIP standards for password length and complexity. Seventh, [REDACTED] updated the [REDACTED] section to include a note that shared accounts must meet NERC-CIP standards for password length and complexity. Eighth, [REDACTED] formalized communications to [REDACTED] Regarding new standards and updated standards to allow [REDACTED] to maintain compliance.

---

<sup>48</sup> CIP-007-6 R5 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

262. On May 26, 2017, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of May 19, 2017. *See Certification of Mitigation Plan Completion, Attachment 85.* On August 16, 2017, ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. *See Mitigation Plan Verification for RFCMIT012746, Attachment 86.*

**K. CIP-009-6 R1 (RFC2016016384)**

263. CIP-009 is designed to recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
264. A violation of CIP-009 R1 has the potential to affect the reliable operation of the BES by preventing or impeding a Registered Entity's response to a Cyber Security Incident.
265. CIP-009-6 R1 states:
- R1.** Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1-Recovery Plan Specifications.
- Part 1.1** Conditions for activation of the recovery plan(s).
- Part 1.2** Roles and responsibilities of responders.
- Part 1.3** One or more processes for the backup and storage of information required to recover BES Cyber System functionality.
- Part 1.4** One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.
- Part 1.5** One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.

*Description of Violation and Risk Assessment*

266. [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-009-6 R1. *See, Self-Report, Attachment 87.* Between September 1, 2015, and December 15, 2015, [REDACTED] implemented [REDACTED] firewalls as part of its plan to divide a [REDACTED]. [REDACTED] had an overarching recovery plan that required the creation of certain recovery procedures; however, during an internal review on September 28, 2016, [REDACTED] discovered that there were no recovery procedures for

the above-referenced firewalls.

267. The major contributing factor to this violation was a process gap. As part of its CIP v5/v6 transition, [REDACTED] implemented a change control process on March 8, 2016, that required the creation of recovery procedures for any new NERC protected assets. However, the firewalls were deployed in the last quarter of 2015 and, therefore, were overlooked when developing recovery procedures. This involves the management practices of asset and configuration management. As part of asset and configuration management, an entity needs to effectively identify and inventory assets and configuration items in order to effectively monitor and maintain control over said assets and items.
268. The violation started on July 1, 2016, when recovery procedures for the firewalls should have been implemented and ended on October 28, 2016, after [REDACTED] created recovery procedures for the firewalls and updated its recovery plan to include the devices.
269. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>49</sup> A lack of preplanned recovery procedures increases the risk of unreliable operation of the BES due to an entity's inability to recover in a timely manner from various hazards affecting BES Cyber Systems. The risk was somewhat mitigated by the fact that [REDACTED] did have vendor-specific recovery procedures available in the event of a failure. Further, [REDACTED] was able to quickly detect and resolve the issue. No harm is known to have occurred.

#### *Mitigating Actions*

270. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-009-6 R1. *See* RFCMIT012374, **Attachment 88**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
271. In the Mitigation Plan, [REDACTED] committed to take the following actions by November 17, 2016. First, [REDACTED] created recovery procedures for the [REDACTED] firewall devices. Second, [REDACTED] updated its recovery plan to include the [REDACTED] firewall devices. Third, [REDACTED] updated the [REDACTED] Checklist to require creation of recovery procedures and updating of the recovery plan for new NERC devices by asset type. Fourth, [REDACTED] confirmed with SMEs that all the assets that need to have a recovery procedure do, in fact, have a recovery procedure.
272. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of November 9, 2016. *See* Certification of Mitigation Plan Completion, **Attachment 89**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. *See* Mitigation Plan Verification for

---

<sup>49</sup> CIP-009-6 R1 has a VRF of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Severe" VSL.

RFCMIT012374, Attachment 90.

**L. CIP-010-2 R1 (RFC2017017546, RFC2017017765, RFC2017017840, RFC2017018307, and RFC2018019647)**

273. CIP-010 safeguards the reliability of the BES by preventing and detecting unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.
274. A violation of CIP-010 R1 has the potential to affect the reliable operation of the BES by permitting a change to be implemented that could adversely affect system security.
275. CIP-010-2 R1 states:
- R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1-Configuration Change Management.
- Part 1.1** Develop a baseline configuration, individually or by group, which shall include the following items:
- 1.1.1** Operating system(s) (including version) or firmware where no independent operating system exists;
  - 1.1.2** Any commercially available or open-source application software (including version) intentionally installed;
  - 1.1.3.** Any custom software installed;
  - 1.1.4.** Any logical network accessible ports; and
  - 1.1.5.** Any security patches applied.
- Part 1.2** Authorize and document changes that deviate from the existing baseline configuration.
- Part 1.3** For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.
- Part 1.4** For a change that deviates from the existing baseline configuration:

- 1.4.1 Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;
- 1.4.2 Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and
- 1.4.3 Document the results of the verification.

**Part 1.5** Where technically feasible, for each change that deviates from the existing baseline configuration:

- 1.5.1 Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and
- 1.5.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

*Description of Violation and Risk Assessment for RFC2017017546*

- 276. [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-010-2 R1 Part 1.1<sup>50</sup>. See, Self-Report, **Attachment 91**. This violation involves two separate instances.
- 277. In the first instance, [REDACTED] discovered that [REDACTED] were deployed to a [REDACTED] ESP even though [REDACTED] did not have a documented baseline configuration as required by CIP-010-2 R1.<sup>51</sup> [REDACTED] failure to follow its documented processes relating to the deployment of Cyber Assets caused several

<sup>50</sup> [REDACTED] initially submitted the Self-Report under CIP-002-5.1 R1. After discussions with [REDACTED] ReliabilityFirst determined that the instance of noncompliance was not a violation of CIP-002-5.1 R1, but, rather, was a violation of CIP-010-2 R1 Part 1.1.

<sup>51</sup> A change order was opened and approved to add the assets in May, 2016. Required approvals were completed by May 17, 2016, and network operations configured [REDACTED] on September 29, 2016. The [REDACTED] were connected to the network that same day, and existing firewall rules permitted remote access to the workstations via [REDACTED] jump server. The consoles were granted access through the firewall to the [REDACTED] networks on October 14, 2016, and to the [REDACTED] network on November 7, 2016.

compliance issues. Specifically, [REDACTED] had not documented a baseline that included any of the information required (CIP-010-2 R1) and did not complete a vulnerability assessment prior to deployment (CIP-010-2 R3). The deployment rendered the ESP undefined, which constituted a violation of CIP-005-5 P 1.1. Additionally, as a result of [REDACTED] failure to follow its documented processes relating to the deployment of Cyber Assets, [REDACTED] failed to enable firewalls (CIP-007-6 P 1.1); failed to identify and evaluate patch sources and apply patches or develop mitigation plans (CIP-007-6 R 2.1 through 2.3); and failed to identify users with access to shared accounts (CIP-007-6 P 5.3).

278. The major contributing factor to the first instance was a lack of documentation and guidance around the issue of deployment of new Cyber Assets into a production environment. There was a lack of coordination between two groups, and change order tasks were assigned to SMEs who were not set up to receive e-mail notification of certain tasks. As a result, the SMEs were not aware of, and did not carry out, the tasks in a timely manner. The issue was discovered when [REDACTED] was conducting a review of change orders more than thirty days old and learned that critical change control and documentation steps were never performed relating to the above-referenced PCAs.
279. In the second instance, on October 17, 2016, a [REDACTED] BCA (an [REDACTED] in the [REDACTED]) failed. Due to the possible impact to BES Cyber System functionality, [REDACTED] immediately replaced the [REDACTED] via its urgent change order process, which allows changes to be carried out without prior approval. However, approval must be obtained the day after the change. The change order was not approved the day after the change due to a lack of a designated manager. This resulted in several compliance issues including: a failure to document a baseline for the server (CIP-010-2 R1); a failure to conduct a vulnerability assessment prior to deployment (CIP-010-2 R3); a failure to identify and evaluate patch sources and apply patches or develop mitigation plans (CIP-007-6 R 2.1 through 2.3); and a failure to identify users with access to shared accounts (CIP-007-6 P 5.3).
280. The major contributing factor to the second instance was process failures. The change process was not set up with an approval manager for the [REDACTED] and there was no escalation step to ensure the change order was approved. The second instance was discovered in February, 2017, during an [REDACTED] review of [REDACTED] asset destruction process.<sup>52</sup>
281. This violation implicates the management practice of asset and configuration management, which requires an entity to effectively identify and inventory asset and configuration items and manage and control changes to said assets and configuration items.

---

<sup>52</sup> An asset was found in a destruction bin located within an [REDACTED], and the logs showed it was properly logged for destruction. However, the related work order did not have a completion date or the required approval recorded.

282. The first instance started on September 29, 2016, when the [REDACTED] were connected to the production environment and ended on March 8, 2017, after all change order steps were completed. The second instance started on October 17, 2016, when the [REDACTED] was deployed and ended on April 3, 2017, after all change order steps were completed.
283. ReliabilityFirst determined that the violation posed a moderate risk to the reliability of the bulk power system based on the following factors.<sup>53</sup> This violation left multiple security gaps open, which could have led to compromise [REDACTED]. The risk was somewhat mitigated by the following facts. First, the entity utilized [REDACTED]. Second, the [REDACTED] were located [REDACTED], and the server was located [REDACTED], thus limiting access to the assets. Further, regarding the server, [REDACTED].

*Mitigating Actions for RFC2017017546*

284. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-010-2 R1. See RFCMIT012908, **Attachment 92**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
285. In the Mitigation Plan, [REDACTED] committed to take the following actions by June 20, 2017: First, [REDACTED] configured its [REDACTED] system to include [REDACTED] SMEs and Managers so that they can receive emails when a work item is assigned. Second, [REDACTED] conducted a deep dive process review to fully understand the operation of the change control process. Third, [REDACTED] obtained all required approvals and perform the required change control measures relating to the issues identified in this violation. Fourth, [REDACTED] documented the process and responsibilities of its various groups installing new assets. Fifth, [REDACTED] updated its [REDACTED] process to include review of open change orders older than thirty days.
286. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of July 17, 2017. See Certification of Mitigation Plan Completion, **Attachment 93**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. See Mitigation Plan Verification for RFCMIT012908, **Attachment 94**.

*Description of Violation and Risk Assessment for RFC2017017765*

287. [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-010-2 R1. See, Self-Report, **Attachment 95**. [REDACTED] discovered that [REDACTED] did not have a documented baseline for a [REDACTED] (a PCA) in violation of CIP-010-2 R1. Then, during an extent of condition review, [REDACTED] found a second [REDACTED].

<sup>53</sup> CIP-010-2 R1 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

NON-PUBLIC AND  
CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED  
FROM THIS PUBLIC VERSION

██████████ without a baseline configuration in violation of CIP-010-2 R1. The first scanner was located at the ██████████ ██████████ ██████████ ██████████ and the second scanner was located in the ██████████ ██████████ ██████████. ██████████ also did not comply with other CIP standards relating to the assets because: the ESP was rendered undefined (CIP-005-5 R1); ██████████ failed to monitor and manage the assets as part of a physical security plan and visitor control program (CIP-006-6 R1 & R2); ██████████ failed to enable only necessary ports (CIP-007-6 R1); ██████████ did not identify and evaluate patch sources and apply patches or develop mitigation plans (CIP-007-6 R 2.1 through 2.3); ██████████ did not deploy methods to deter, detect, or prevent malicious code (CIP-007-6 R3); ██████████ did not configure security event monitoring (CIP-007-6 R4); ██████████ did not identify and inventory all default account types, identify users with access to shared accounts, or implement other system access controls (CIP-007-6 R5); ██████████ did not perform a vulnerability assessment prior to deployment (CIP-010-2 R3); ██████████ failed to comply with transient cyber assets and removable media standards (CIP-010-2 R4); and ██████████ failed to utilize required information protection procedures and failed to take necessary actions to prevent unauthorized retrieval of information (CIP-011-2 R1 through R2).

288. The major contributing factors to this violation were process gaps and oversight by responsible personnel. The ██████████ were implemented prior to CIP v5/v6 and were missed as part of ██████████ v5/v6 migration. Responsible personnel did not adequately inventory assets, and certain processes did not catch the issue. This implicates the management practice of asset and configuration management, which requires an entity to effectively identify and inventory assets and configuration items. It also implicates the management practice of workforce management, which includes the effective management and training of staff in support of their roles.
289. The violation started on July 1, 2016, when ██████████ failed to comply with various standards relating to the assets, and ended on June 30, 2017, when ██████████ brought the assets into compliance.
290. ReliabilityFirst determined that the violation posed a moderate risk to the reliability of the bulk power system based on the following factors.<sup>54</sup> Failing to apply baseline configuration controls to PCAs and the resulting failure to comply with other CIP standards (patching, etc.) could lead to compromise of the PCAs and a failure to identify real security events, which could allow a bad actor to carry out malicious activities undetected. The risk was somewhat mitigated by the fact that ██████████ ██████████ and access was controlled and limited to trained SMEs. The risk was further mitigated because the ██████████ is a security hardened appliance, and it cannot be accessed from the network using ██████████ ██████████. Rather, it can only be accessed via the ██████████ m ██████████, and only a limited number of administrators have access to the appliance via the

---

<sup>54</sup> CIP-010-2 R1 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.



console. No harm is known to have occurred.

*Mitigating Actions for RFC2017017765*

291. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-010-2 R1. See RFCMIT013013, **Attachment 96**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
292. In the Mitigation Plan, [REDACTED] committed to take the following actions by June 30, 2017: First, [REDACTED] brought both devices into, or confirm, and documented compliance with the [REDACTED] NERC CIP requirements. Second, [REDACTED] updated the [REDACTED] to include [REDACTED] assets.
293. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of June 30, 2017. See Certification of Mitigation Plan Completion, **Attachment 97**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. See Mitigation Plan Verification for RFCMIT013013, **Attachment 98**.

*Description of Violation and Risk Assessment for RFC2017017840*

294. [REDACTED], [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-010-2 R1. See, Self-Report, **Attachment 99**. [REDACTED], [REDACTED] discovered that personnel were not documenting the results of required cyber security controls testing and verifications when performing non-routine configuration changes at the [REDACTED] ([REDACTED]). These changes were completed outside of the documented routine patching process and included software updates and installations on various assets.<sup>55</sup>
295. The major contributing factors to this violation were a failure to follow an established process and deficient work instructions. There was no instruction at the SME level specifying roles and responsibilities for configuration change management, including documenting the results of cyber security control testing and verification for non-routine configuration changes. This implicates the management practice of workforce management. Workforce management includes promoting awareness and providing training to impart skills and knowledge to enable personnel to perform specific reliability and resilience functions. It is also important for an entity to implement well defined and executable processes and procedures to minimize the frequency of errors committed by responsible personnel.
296. The violation started on July 1, 2016, was required to document the results of verifications and ended on August 31, 2017, after [REDACTED] corrected the issue.
297. ReliabilityFirst determined that the violation posed a minimal risk to the reliability

---

<sup>55</sup> Specifically, pursuant to [REDACTED], [REDACTED] updated/installed [REDACTED] affecting [REDACTED] assets.

of the bulk power system based on the following factors.<sup>56</sup> Failing to adequately oversee and document changes reduces an entity's ability to detect unauthorized changes that could lead to misoperation or instability in the BES. However, that risk was mitigated by the following factors. This was primarily a documentation issue, as the entity complied with all other requirements to carry out the changes. Further, the affected assets were up-to-date with regards to patching, and no adverse impact is known to have occurred.

*Mitigating Actions for RFC2017017840*

298. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-010-2 R1. See RFCMIT013022-1, **Attachment 100**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
299. In the Mitigation Plan, [REDACTED] committed to take the following actions by September 8, 2017. First, [REDACTED] developed a testing template to document CIP-005 and CIP-007 changes. This will verify that the required documentation is completed. Second, [REDACTED] sent an email to all NERC SMEs reminding them of the requirement to document non-routine configuration changes. Third, [REDACTED] verified that security controls (CIP-005 and CIP-007) for each asset were still active and in place. Fourth, [REDACTED] communicated the developed [REDACTED] in a staff meeting. Fifth, [REDACTED] developed a [REDACTED] directed to the point of activity for the SMEs performing CIP-010 R1 P1.4 tasks. Sixth, [REDACTED] sent out a communication regarding the testing template directed to the point of activity for the SMEs performing CIP-010 R1 P1.4 tasks. Seventh, [REDACTED] added a requirement to complete the testing template as a control to the [REDACTED] process and communicate this fact to all SMEs.
300. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of August 31, 2017. See Certification of Mitigation Plan Completion, **Attachment 101**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. See Mitigation Plan Verification for RFCMIT013022-1, **Attachment 102**.

*Description of Violation and Risk Assessment for RFC2017018307*

301. On September 5, 2017, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-010-2 R1. See, Self-Report, **Attachment 103**. Specifically, backup software was inappropriately installed on [REDACTED] without proper authorization and testing.
302. As background, first, four change orders were created to install system backup software ([REDACTED] on non-NERC assets. An [REDACTED] recognized [REDACTED] of the listed [REDACTED] as NERC assets and, therefore, excluded the servers from the original change orders. Several months after the change orders

---

<sup>56</sup> CIP-010-2 R1 has a VRF of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Severe" VSL.

were completed and closed, a member of [REDACTED] team ran a maintenance monitoring report and discovered [REDACTED] running [REDACTED] software. The server engineer wrongly assumed that the [REDACTED] were supposed to be running [REDACTED] per the original change orders, so he proceeded to install [REDACTED] on the [REDACTED] on July 20, 2017. The issue was discovered seven days later during a scan to generate a configuration monitoring report after a [REDACTED] had been installed on [REDACTED] (including the [REDACTED] that recently had [REDACTED] installed on them) and [REDACTED].

303. The major contributing factor to this violation was a failure to follow a documented process, which implicates the management practice of workforce management. The server engineer did not have an authorized change order before proceeding to install the new backup software on the [REDACTED]; rather, he worked off an incorrect assumption. Workforce management includes the need to effectively train personnel and reinforce the existence and importance of established processes and procedures.
304. The violation started on July 20, 2017, when the server engineer installed the software and ended on September 11, 2017, after [REDACTED] obtained the necessary authorizations and completed the necessary testing of the software.
305. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>57</sup> Any time new or updated software is introduced without authorization or testing, there is an increased risk of unintended consequences, including loss of the affected assets. Here, the issue only affected [REDACTED] for a short period of time. The risk was further mitigated because the backup software had already been installed on several non-NERC assets, which did not experience any issues due to the installation. Lastly, the old backup software was left on the [REDACTED], thus further reducing the risk.

*Mitigating Actions for RFC2017018307*

306. On October 2, 2017, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-010-2 R1. See RFCMIT013267, **Attachment 104**. On October 27, 2017, ReliabilityFirst accepted the Mitigation Plan.
307. In the Mitigation Plan, [REDACTED] committed to take the following actions by November 6, 2017. First, [REDACTED] served a disciplinary action to the employee in [REDACTED] for not following the defined and documented change control process. Second, [REDACTED] created a retroactive change order to install [REDACTED] on the production [REDACTED] and have it approved by the [REDACTED] with an appropriate explanation of the incident. Third, [REDACTED] re-emphasized the change control procedures and protocols to the [REDACTED] team. Fourth, [REDACTED]

---

<sup>57</sup> CIP-010-2 R1 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

created a checklist to serve as a quick reference to the existing change control process.

308. On November 6, 2017, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of November 2, 2017. *See* Certification of Mitigation Plan Completion, **Attachment 105**. On November 28, 2017, ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. *See* Mitigation Plan Verification for RFCMIT013267, **Attachment 106**.

*Description of Violation and Risk Assessment for RFC2018019647*

309. On April 25, 2018, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-010-2 R1. *See*, Self-Report, **Attachment 107**. During the planning phase to upgrade its [REDACTED] for an updated application ([REDACTED]) a SME identified the planned systems as [REDACTED]. Then, [REDACTED] realized that the existing systems also should have been identified as [REDACTED] but they were not. The existing [REDACTED] were implemented in October, 2012, and were never classified as NERC assets.<sup>58</sup> The [REDACTED] are [REDACTED], which are configured to [REDACTED] from [REDACTED] and [REDACTED]. The [REDACTED] system consists of a [REDACTED]. The system [REDACTED] to [REDACTED] which [REDACTED] uses as a [REDACTED] tool.

310. As a result of the foregoing, [REDACTED] did not have documented baselines for the [REDACTED] in violation of CIP-010-2 R1. Additionally, [REDACTED] did not comply with numerous other CIP standards relating to the assets because: the ESP was rendered undefined (CIP-005-5 R1); [REDACTED] failed to adequately manage interactive remote access (CIP-005-5 R2); [REDACTED] failed to monitor and manage the assets as part of a physical security plan and visitor control program (CIP-006-6 R1 & R2); [REDACTED] failed to enable only necessary ports (CIP-007-6 R1); [REDACTED] did not identify and evaluate patch sources and apply patches or develop mitigation plans (CIP-007-6 R 2.1 through 2.3); [REDACTED] did not deploy methods to deter, detect, or prevent malicious code (CIP-007-6 R3); [REDACTED] did not configure security event monitoring (CIP-007-6 R4); [REDACTED] did not identify and inventory all default account types, identify users with access to shared accounts, or implement other system access controls (CIP-007-6 R5); and [REDACTED] did not have a documented recovery plan (CIP-009-6 R1).

311. The major contributing factor to this violation was deficient processes and procedures, which created a significant delay in identifying and protecting the [REDACTED] [REDACTED]. This violation implicates the management practices of asset and configuration management and workforce management. Asset and configuration

<sup>58</sup> [REDACTED] missed multiple opportunities to identify and classify the [REDACTED] as [REDACTED] including the CIP v5/v6 transition and the [REDACTED] implementation. The [REDACTED] servers act as [REDACTED] of the [REDACTED]. The [REDACTED] was identified and treated as a NERC asset since the date of its implementation.



316. On October 19, 2018, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of October 16, 2018. *See* Certification of Mitigation Plan Completion, **Attachment 109**. On November 19, 2018, 2018, ReliabilityFirst verified [REDACTED] completed the Mitigation Plan on October 18, 2018. *See* Mitigation Plan Verification for RFCMIT013784-1, **Attachment 110**.

**M. CIP-010-2 R3 (RFC2017017836, RFC2017018498, and RFC2018019048)**

317. CIP-010 safeguards the reliability of the BES by preventing and detecting unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

318. A violation of CIP-010 R3 has the potential to affect the reliable operation of the BES by inhibiting Registered Entities' ability to identify potential vulnerabilities in their cyber security programs.

319. CIP-010-2 R3 states:

**R3.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3-Vulnerability Assessments.

**Part 3.1** At least once every 15 calendar months, conduct a paper or active vulnerability assessment.

**Part 3.2** Where technically feasible, at least once every 36 calendar months:

**Part 3.2.1** Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and

**Part 3.2.2** Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

**Part 3.3** Prior to adding a new applicable Cyber Asset to a production

environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.

**Part 3.4** Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.

*Description of Violation and Risk Assessment for RFC2017017836*

320. [REDACTED], [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-010-2 R3. *See*, Self-Report, **Attachment 111**. During an internal [REDACTED] in March, 2017, [REDACTED] discovered that between July 1, 2016, and March, 2017, it did not perform active vulnerability assessments of [REDACTED] assets (i.e., [REDACTED],<sup>60</sup> [REDACTED] servers, [REDACTED] [REDACTED], [REDACTED] and [REDACTED] prior to deploying said assets into a [REDACTED] (i.e., [REDACTED]).
321. The major contributing factor to this violation was a deficient procedure. [REDACTED] implemented a program that included a [REDACTED] component, which required a vulnerability assessment to be performed prior to deploying an asset to a [REDACTED]. However, [REDACTED] had never established any formal and specific procedures regarding when or how to perform active vulnerability assessments. This implicates the management practice of workforce management. Workforce management includes the need to manage systems in a way that minimizes human factor issues, which can oftentimes be accomplished through the implementation of clear and executable procedures.
322. The violation started on July 1, 2016, when [REDACTED] began introducing assets into a production environment prior to conducting active vulnerability assessments and ended on May 25, 2017, after [REDACTED] completed remediation efforts.
323. ReliabilityFirst determined that the violation posed a moderate risk to the reliability of the bulk power system based on the following factors.<sup>61</sup> The risks in this case are (a) the increased likelihood of introducing security vulnerabilities and (b) the increased likelihood of significant delays in addressing said vulnerabilities. The risks were somewhat mitigated by the following factors. The assets were located within [REDACTED] and were subject to additional security controls (e.g., [REDACTED]).

<sup>60</sup> The [REDACTED] were ultimately disabled and removed from production.

<sup>61</sup> CIP-010-2 R3 has a VRF of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Severe" VSL.

[REDACTED], the [REDACTED]  
[REDACTED]). It is also worth noting that after-the-fact vulnerability assessments showed that no vulnerabilities existed. No harm is known to have occurred.

*Mitigating Actions for RFC2017017836*

324. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-010-2 R3. See RFCMIT013048, **Attachment 112**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
325. In the Mitigation Plan, [REDACTED] committed to take the following actions by November 30, 2017. First, [REDACTED] performed an extent of condition on all assets added to [REDACTED] between July 1, 2016, and July 1, 2017. Second, [REDACTED] ensured that all assets added within the production environment went through a vulnerability assessment. Third, [REDACTED] created a new NERC CIP assets onboarding process to ensure compliance with NERC CIP standards. Fourth, [REDACTED] updated its [REDACTED] process to check verification of new assets added to production based on the new onboarding process. Fifth, [REDACTED] communicated the newly developed [REDACTED] and updated [REDACTED] process to the SMEs.
326. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan. See Certification of Mitigation Plan Completion, **Attachment 113**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan as of November 16, 2017. See Mitigation Plan Verification for RFCMIT013048, **Attachment 114**.

*Description of Violation and Risk Assessment for RFC2017018498*

327. On October 17, 2017, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-010-2 R3. See, Self-Report, **Attachment 115**. In January, 2017, [REDACTED] began [REDACTED] installations, and [REDACTED] were in scope for said installations.<sup>62</sup> Then, on September 6, 2017, [REDACTED] thought that it discovered evidence that [REDACTED] equipment had been plugged into a [REDACTED] ESP prior to the performance of a vulnerability assessment. During further review on September 22, 2017, [REDACTED] determined that installations had been performed in the [REDACTED] and [REDACTED] networks for the [REDACTED] but not within a [REDACTED] ESP.<sup>63</sup> However, [REDACTED] opted to conduct an extent of condition of possible installations of [REDACTED] equipment prior to the performance of a vulnerability assessment in [REDACTED]. During this review, [REDACTED] discovered that [REDACTED] and [REDACTED] assets were added to the production environment of [REDACTED]

<sup>62</sup> Specifically, the installations affected [REDACTED] and [REDACTED]

<sup>63</sup> Regardless, this would have affected a [REDACTED] (i.e., CIP-010-2 P 3.3 did not require an active vulnerability assessment prior to adding assets to the production environment).





requirements for [REDACTED] assets.

333. On January 18, 2018, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of January 17, 2018. See Certification of Mitigation Plan Completion, **Attachment 117**. On August 22, 2018, ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. See Mitigation Plan Verification for RFCMIT013394-1, **Attachment 118**.

*Description of Violation and Risk Assessment for RFC2018019048*

334. On January 10, 2018, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-010-2 R3. See, Self-Report, **Attachment 119**. Specifically, [REDACTED] did not complete a paper assessment or an active vulnerability assessment of [REDACTED] production assets within the 15 calendar month constraints of CIP-010-2 P 3.1. [REDACTED] discovered the issue when examining evidence for a separate issue.
335. The major contributing factor to this violation was a misunderstanding by personnel performing vulnerability management functions. The [REDACTED] team was performing active vulnerability assessments in a test environment in accordance with CIP-010-2 P 3.2 and mistakenly assumed that these assessments would also fulfill the requirements of CIP-010-2 P 3.1.<sup>65</sup>
336. This violation implicates the management practice of workforce management. Workforce management includes training personnel and providing the tools necessary to ensure that said personnel understand and execute their security and reliability functions.
337. The violation started on May 25, 2017, when [REDACTED] failed to conduct paper or active vulnerability assessments and ended on January 26, 2018, after [REDACTED] remedied the issue.
338. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>66</sup> The risk of failing to perform vulnerability assessments is the increased likelihood of failing to identify a weakness that an attacker could exploit, thereby allowing that vulnerability to persist. The risk was mitigated by the following factors. [REDACTED] utilizes multiple security controls including [REDACTED]. These controls minimize attack vectors for any vulnerabilities that may exist in [REDACTED] environment. Further, [REDACTED] had been performing thorough assessments in a test environment, which was designed to

---

<sup>65</sup> The scanning tool was known to cause operational issues in the production environment. And, the SMEs performing the assessments assumed that the test environment assessments were sufficient because the scanning tool modeled the baseline configuration of the production assets.

<sup>66</sup> CIP-010-2 R3 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Moderate” VSL.

represent the production environment, thereby further reducing the risk.

*Mitigating Actions for RFC2018019048*

339. On January 29, 2018, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-010-2 R3. See RFCMIT013546, **Attachment 120**. On February 23, 2018, ReliabilityFirst accepted the Mitigation Plan.
340. In the Mitigation Plan, [REDACTED] committed to take the following actions by April 30, 2018. First, [REDACTED] conducted a vulnerability assessment on all production assets not scanned during the yearly assessment. Second, [REDACTED] revised the program document governing vulnerability assessments to provide clarification for SMEs that the CIP-010 P 3.1 and P 3.2 standards are separate. Third, [REDACTED] utilized the required reading program to verify that all SMEs working with [REDACTED] ESPs have read and understood the requirements. Fourth, [REDACTED] updated the [REDACTED] to include annual completion of CIP010 P 3.1 requirements and, [REDACTED], completion of CIP010 P 3.2. Fifth, [REDACTED] conducted an extent of condition to verify assets without paper or active assessment did not exist for other NERC ESPs.
341. On April 30, 2018, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of April 30, 2018. See Certification of Mitigation Plan Completion, **Attachment 121**. On September 6, 2018, ReliabilityFirst verified [REDACTED] completed this Mitigation Plan on May 1, 2018. See Mitigation Plan Verification for RFCMIT013546, **Attachment 122**.

**N. CIP-010-2 R4 (RFC2017018285 and RFC2017018761)**

342. CIP-010 increases the reliability of the BES by preventing and detecting unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.
343. A violation of CIP-010 R4 has the potential to affect the reliable operation of the BES by allowing potential compromise of systems through Transient Cyber Assets or Removable Media that are not fully protected.
344. CIP-010-2 R4 states:
  - R4.** Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.

*Description of Violation and Risk Assessment for RFC2017018285*

345. On August 24, 2017, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-010-2 R4. *See*, Self-Report, **Attachment 123**. On or about May 17, 2017, a firmware update provided by a vendor inadvertently changed the password of a [REDACTED] [REDACTED] to a previously used password.<sup>67</sup> After the change, an [REDACTED] representative was unable to log into the [REDACTED] and a ticket was opened with the vendor [REDACTED]. The vendor recommended that [REDACTED] attempt to log directly into the [REDACTED] switch with a console, so [REDACTED] [REDACTED] “crash cart” for troubleshooting. He wrongly assumed that the laptop was an authorized Transient Cyber Asset (“TCA”). He connected the laptop, but his login attempts failed. The vendor asked him to leave the laptop connected until a technician arrived. The technician arrived on May 19, 2017, and was not able to log into the switch. Thereafter, the technician and [REDACTED] personnel forgot to disconnect the laptop. It remained connected until June 20, 2017, when it was discovered during a [REDACTED]. The laptop was not an authorized TCA. It was a [REDACTED] machine with no network connection and an unknown patch and antivirus update history.
346. The major contributing factors to this violation were deficient practices and procedures. The SME wrongly assumed that he could use the laptop from the [REDACTED] [REDACTED]. This was precipitated by the following facts: the [REDACTED] team had not previously been assigned a TCA;<sup>68</sup> many groups had access to the [REDACTED] and there was no distinguishing mark on the laptop used by the SME (e.g., “DO NOT USE FOR NERC CIP”). This implicates the management practice of workforce management, which includes the need to train personnel and implement practices and procedures that minimize human factor issues such as the one that occurred in this case.
347. The violation started on May 17, 2017, when [REDACTED] connected the unauthorized TCA and ended on June 20, 2017, when [REDACTED] disconnected the machine.
348. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>69</sup> Connecting unauthorized TCAs for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting increases the likelihood that such TCAs will be used as vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. The risk was somewhat mitigated because the two individuals using the unauthorized TCA could not log into [REDACTED] [REDACTED] due to the unknown password change, thereby reducing their ability to

---

<sup>67</sup> The [REDACTED] [REDACTED] is associated with [REDACTED] [REDACTED] and, as such, is not directly used for the operation of the BES. It is classified as a [REDACTED]

<sup>68</sup> [REDACTED] had a program governing TCAs and Removable Media; however, the [REDACTED] team did not have authorized TCA users or devices.

<sup>69</sup> CIP-010-2 R4 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

transfer code or change settings from the laptop. The [REDACTED] [REDACTED] patches were up-to-date, and baseline monitoring would have detected any changes if an unidentified vulnerability had been exploited via new software being added while the laptop was connected. Further, the asset is not directly used for operation of the BES, and it was not in an operating state (i.e., the asset was down) while the presumed TCA was connected. And, the connection was serial, thus reducing the probability of malicious software being transferred.

*Mitigating Actions for RFC2017018285*

349. On September 21, 2017, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-010-2 R4. See RFCMIT013252, **Attachment 124**. On October 10, 2017, ReliabilityFirst accepted the Mitigation Plan.
350. In the Mitigation Plan, [REDACTED] committed to take the following actions by October 20, 2017. First, [REDACTED] created a list of requirements for an [REDACTED] TCA. Second, [REDACTED] investigated the unauthorized TCA from [REDACTED] to determine if it was needed for NERC-CIP support. Third, [REDACTED] created a list of [REDACTED] users that needed access to a TCA. Fourth, [REDACTED] communicated the program to NERC-CIP SMEs. Fifth, [REDACTED] determined what device meets the requirements for [REDACTED]. Sixth, [REDACTED] added this possible noncompliance to the [REDACTED]. Seventh, [REDACTED] implemented a TCA solution made in Milestone #3. Eighth, [REDACTED] communicated with required feedback to NERC-CIP SMEs with access to TCAs.
351. On October 18, 2017, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of October 13, 2017. See Certification of Mitigation Plan Completion, **Attachment 125**. On November 28, 2017, ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. See Mitigation Plan Verification for RFCMIT013252, **Attachment 126**.

*Description of Violation and Risk Assessment for RFC2017018761*

352. On December 5, 2017, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-010-2 R4. See, Self-Report, **Attachment 127**. In October, 2017, an employee did not follow proper procedures for connecting a TCA within a protected ESP at the [REDACTED]. More specifically, the employee did not collect appropriate evidence.
353. As background, On October 19, 2017, a specialist from the [REDACTED] received a call from [REDACTED] reporting a [REDACTED]. The next day, on October 20, 2017, a new [REDACTED], and a TCA was used to program it. However, despite the new installation, the [REDACTED], so on October 23, 2017, [REDACTED] was re-installed, and the [REDACTED] specialist and an [REDACTED] specialist working on this issue mistakenly concluded that no NERC work/documentation was needed for these activities. The above-referenced

new module was programmed using a SME's corporate computer, which [REDACTED] intended to designate as a TCA. However, the laptop was never included on the list of authorized TCAs. A [REDACTED] at the [REDACTED] [REDACTED] discovered the non-compliance on October 23, 2017.

354. The major contributing factor to this violation was inadequate training. The SME was not aware of the TCA program and procedures. This implicates the management practice of workforce management, which includes the need to effectively train personnel to minimize preventable mistakes.
355. The violation started on October 20, 2017, when the TCA procedure was not followed and ended on December 19, 2017, after [REDACTED] remediated the issue.
356. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>70</sup> Introducing a TCA to a CIP environment without following proper procedures could lead to the propagation of malware within the ESP and a corresponding adverse effect on the BES. The risk was mitigated by the short duration of the connection as well as the fact that the laptop had up-to-date virus and patching controls. An after-the-fact baseline confirmed that there was no adverse impact to the BES. This violation was really a documentation issue because the TCA was supposed to be on the authorized TCA list.

*Mitigating Actions for RFC2017018761*

357. On December 14, 2017, [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-010-2 R4. *See* RFCMIT013445, **Attachment 128**. On January 10, 2018, ReliabilityFirst accepted the Mitigation Plan.
358. In the Mitigation Plan, [REDACTED] committed to take the following actions by December 22, 2017. First, [REDACTED] conducted training for all [REDACTED] SMEs on the TCA process. Second, [REDACTED] prepared a retroactive change order to explain the work performed and update the documentation. Immediate containment action involved submitting this change order and running a new baseline to verify that the new module did not make any adverse changes. This process included the creation of a test rack that was used to install the new module by resetting it back to the original factory settings.
359. On January 17, 2018, [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan. *See* Certification of Mitigation Plan Completion, **Attachment 129**. On April 11, 2018, ReliabilityFirst verified [REDACTED] completed this Mitigation Plan as of February 6, 2018. *See* Mitigation Plan Verification for RFCMIT013445, **Attachment 130**.

---

<sup>70</sup> CIP-010-2 R4 has a VRF of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Severe" VSL.

**O. CIP-011-2 R1 (RFC2017017838)**

360. CIP-011 safeguards the reliability of the Bulk-Power System by preventing unauthorized access to BES Cyber System information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
361. A violation of CIP-011 R1 has the potential to affect the reliable operation of the BES by allowing bad actor access to BES Cyber System information and compromising BES safety.
362. CIP-011-2 R1 states:
- R1.** Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1-Information Protection.
- Part 1.1** Method(s) to identify information that meets the definition of BES Cyber System Information.
- Part 1.2** Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.

*Description of Violation and Risk Assessment*

363. [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] it was in violation of CIP-011-2 R1. See, Self-Report, **Attachment 131.** [REDACTED] upgraded to [REDACTED] between December, 2016, and February, 2017. The [REDACTED] included a [REDACTED]. On April 17, 2017, [REDACTED] used a [REDACTED] to scan [REDACTED] for BCSI in the [REDACTED].<sup>71</sup> The scan found [REDACTED] instances of potential BCSI documentation stored in [REDACTED] locations. During further review, [REDACTED] determined that only [REDACTED] of the [REDACTED] documents contained BCSI. More specifically, the documents contained [REDACTED]. The [REDACTED] locations were not accounted for as a BCSI storage area, and the BCSI therein was not identified or adequately protected in violation of CIP-011-2 R1.
364. The major contributing factor to this violation was inadequate planning. The operating system upgrade process did not include an assessment of potential changes to default settings, such as save settings. This implicates the management practice of planning, which includes the need to effectively identify project risks and establish safeguards to avoid an unintentional adverse effect on BES reliability

---

<sup>71</sup> The scan searched for files with the phrases [REDACTED] and [REDACTED]

and resilience.

365. The violation started on December 1, 2016, when the [REDACTED] was changed and ended on June 22, 2017, after [REDACTED] finished removing the BCSI documents from the [REDACTED] [REDACTED]
366. ReliabilityFirst determined that the violation posed a minimal risk to the reliability of the bulk power system based on the following factors.<sup>72</sup> Failing to identify BCSI and BCSI storage locations could lead to unauthorized access to BCSI and a corresponding dissemination or use thereof. The risk was somewhat mitigated by the following facts. [REDACTED] access was restricted to [REDACTED] personnel, and the [REDACTED] storage locations [REDACTED]. Restated, the risk was reduced because access to specific BCSI was limited to [REDACTED]. Further, the documents were immediately quarantined by the [REDACTED], which rendered the documents inaccessible during the period while [REDACTED] was removing them.

#### *Mitigating Actions*

367. On [REDACTED], [REDACTED] submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-011-2 R1. See RFCMIT013012, **Attachment 132**. On [REDACTED], ReliabilityFirst accepted the Mitigation Plan.
368. In the Mitigation Plan, [REDACTED] committed to take the following actions by June 30, 2017. First, [REDACTED] configured the [REDACTED] for [REDACTED] monitoring and quarantining of NERC CIP documents. Second, [REDACTED] updated the [REDACTED] [REDACTED] to state that storage on [REDACTED] and [REDACTED] is prohibited. Third, [REDACTED] communicated the update across the [REDACTED]. Fourth, [REDACTED] verified that any files in [REDACTED] and [REDACTED] that contained BCSI had been removed or deleted.
369. On [REDACTED], [REDACTED] certified to ReliabilityFirst that it completed this Mitigation Plan as of June 30, 2017. See Certification of Mitigation Plan Completion, **Attachment 133**. On [REDACTED], ReliabilityFirst verified [REDACTED] completion of this Mitigation Plan. See Mitigation Plan Verification for RFCMIT013012, **Attachment 134**.

---

<sup>72</sup> CIP-011-2 R1 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.



## Attachment 2

## Record documents for the violation of CIP-002-5.1 R1

- 2.a The Entity's Self-Report (RFC2017018708);
- 2.b The Entity's Mitigation Plan designated as RFCMIT013479 submitted [REDACTED];
- 2.c The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
- 2.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED]

Self Report

Entity Name: [REDACTED]

NERC ID: [REDACTED]

Standard: CIP-002-5.1

Requirement: CIP-002-5.1 R1.

Date Submitted: November 21, 2017

Has this violation previously No  
been reported or discovered?:

Entity Information:

Joint Registration  
Organization (JRO) ID:

Coordinated Functional  
Registration (CFR) ID:

Contact Name: [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: October 17, 2016

End/Expected End Date:

Reliability Functions: [REDACTED]

Is Possible Violation still No  
occurring?:

Number of Instances: 1

Has this Possible Violation No  
been reported to other  
Regions?:

Which Regions:

Date Reported to Regions:

Detailed Description and \*Detailed Description:  
Cause of Possible Violation:

[REDACTED]

What is the problem?

[REDACTED]

Self Report

[REDACTED] This is in violation of CIP-002 R1.

Root Cause of Possible Violation:

The root cause of this possible violation is: Our existing [REDACTED] tests appear to lack effectiveness in [REDACTED] process to detect changes in our environment as we bring new [REDACTED]. Further investigation during mitigation planning will refine the root cause.

How was the violation discovered?

The violation was discovered during a design session for the new [REDACTED], it was noted that [REDACTED]. On Monday 10/16/17, a list was provided currently showing the [REDACTED]. Currently [REDACTED]. With this change in understanding, [REDACTED] is not classified correctly and hence is a violation of CIP002.

\*Explain how is it determined that the Noncompliance is related to documentation, performance, or both.

[REDACTED]

\*Timeline:

In April 19, 2016, the [REDACTED]. The assessment defined the [REDACTED]. This assessment was in preparation for the inclusion of [REDACTED] under the NERC CIP regulations.

On October 17, 2016, the [REDACTED]

December 2016: Held [REDACTED] CIP-002 [REDACTED] of BES Assets. The result was to defined both [REDACTED] as [REDACTED] and [REDACTED] primary also remain classified as [REDACTED]. No reassessment was completed on the [REDACTED] since no change was identified which would cause a re-review.

January 23 - 24, 2017: 2017 [REDACTED]. This meets our CIP 002 "annual or every 15 months" assessment. Results re-affirmed [REDACTED]

[REDACTED] CIP-002 [REDACTED] that:

[REDACTED] would be moved from [REDACTED] to [REDACTED] to [REDACTED], rather than making [REDACTED]. During this assessment, it was decided to hold an [REDACTED] scheduled 2017 [REDACTED] on [REDACTED] (January 23-24, 2017), to ensure [REDACTED] classified as soon as it was identified as a candidate BES Asset to maintain it still met CIP-002 Compliance requirements. No reassessment was completed on the primary site, since no change was identified which would cause a re-review.

[REDACTED]

Self Report

[REDACTED]

Mitigating Activities:

Description of Mitigating Immediate Correcting Activities:

Activities and Preventative • The immediate corrective action that has taken place is that the [REDACTED]

Measure: [REDACTED]  
[REDACTED]  
This removes [REDACTED]  
[REDACTED]

Mitigating Activities:

• Mitigation Activities have already been put in place as of November 14th, 2017 to reclassify the [REDACTED] back to a [REDACTED]

[REDACTED] This moves the [REDACTED]  
[REDACTED]

Preventative Measures:

• Formally add a [REDACTED] CIP-002 [REDACTED]  
[REDACTED] to related [REDACTED]  
[REDACTED] This is done out-of-band  
of [REDACTED]  
[REDACTED] (as changes occur), as well as during this [REDACTED]  
(to re-affirm changes assessments).

Date Mitigating Activities Completed: [REDACTED] [REDACTED] has  
been removed from the [REDACTED] and moved to [REDACTED] on [REDACTED]  
[REDACTED] This moves the [REDACTED] back to a [REDACTED]  
[REDACTED]

Date Mitigating Activities  
Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Moderate

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: The potential impact to the BES was Moderate, since the [REDACTED] was  
managing [REDACTED]  
[REDACTED] causing an elevated risk to the BES.

The actual impact to the BES is low, because the [REDACTED] [REDACTED]  
[REDACTED] This significantly reduces the  
[REDACTED] the [REDACTED] is [REDACTED]  
[REDACTED], so the [REDACTED]  
[REDACTED] This also brings [REDACTED] back into  
compliance with the CIP002 standard.

Risk Assessment of Impact to BPS: The risk assessment of impact to the BES is low. As of November 14th, 2017,  
the [REDACTED] is once again managing [REDACTED]  
[REDACTED]

Self Report

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

## Mitigation Plan

### Mitigation Plan Summary

Registered Entity: [REDACTED]

Mitigation Plan Code:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017018708	CIP-002-5.1 R1.	

Mitigation Plan Submitted On: January 03, 2018

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: April 09, 2018

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [REDACTED] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

## Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

- (1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
  - (2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
  - (3) The cause of the Alleged or Confirmed Violation(s).
  - (4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
  - (5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
  - (6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
  - (7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
  - (8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
  - (9) Any other information deemed necessary or appropriate.
  - (10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
  - (11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.
- The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.
  - This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.
  - If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.
  - Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.
  - Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.
  - The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [REDACTED]

NERC Compliance Registry ID: [REDACTED]

Address: [REDACTED]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [REDACTED] [REDACTED]

Title: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]



Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017018708	10/17/2016	CIP-002-5.1 R1.
Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:[See Standard for sub-req's]		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

Brief Description: (What happened?)

On 10/13/2017

[Redacted]

Subsequent to this finding, a plan was defined and implemented where [Redacted]

Cause: (what caused the violation?)

[Redacted]

Several untracked changes brought [Redacted] In addition, no controls were added or modified to subsequently address the application of additional requirements to the Asset [Redacted]

How was the violation discovered?

The violation was discovered during a [Redacted]

Results of the RCA: (What is the root cause?)

The root cause of this possible violation is: Changes to our environment were not identified through the [Redacted] process. No controls exist within this process to holistically identify and hand-off changes that may impact the compliance posture of [Redacted] to the CIP-002 formalized process for assessment and re-classification.

Relevant information regarding the identification of the violation(s):

The violation was discovered during [Redacted], it was noted that the [Redacted] was [Redacted] On Monday 10/16/17, a list was provided currently showing that [Redacted]

Currently [Redacted] is listed on the CIP 002 list as [Redacted] location and not under compliance. With this change in understanding, [Redacted] is not classified correctly and hence is a violation of CIP002.

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

Milestone 1 - The immediate corrective action that has taken place is that the [REDACTED] has been removed from the [REDACTED] and moved to the [REDACTED] as of [REDACTED]. This removes [REDACTED]. The evidence will be the updated [REDACTED] from previously [REDACTED] to [REDACTED] along with SME comments.

Milestone 2 - To prevent this from occurring in the future, [REDACTED] will modify the [REDACTED]. The evidence will be an updated process.

Milestone 3 - Update the CIP 002 Program to include: For the [REDACTED], the CIP-002 Program will be modified to include a formal review of the change documentation from the [REDACTED] (Milestone 2) as well as current [REDACTED]. Currently this process is not formalized. This evidence will be update CIP-002 program that will include a formal review of the changed documentation from the [REDACTED] as well as [REDACTED].

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: April 09, 2018

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
1. [REDACTED]	[REDACTED]	11/14/2017	11/14/2017		No
2. Add a review/escalation process to [REDACTED]	Modify the existing [REDACTED] by adding a [REDACTED]	02/06/2018			No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED] on evaluation.</p>				
<p>3. Add formal [REDACTED] process in CIP-002 [REDACTED]</p>	<p>For the [REDACTED], the CIP-002 Program will be modified to include a formal review of the change documentation from the [REDACTED] (Milestone 2) as well as [REDACTED] as part of the [REDACTED]</p>	<p>04/09/2018</p>			<p>No</p>

Additional Relevant Information

The immediate corrective action that has taken place is that the [REDACTED]

The remaining milestones intended to address avoidance of a reoccurrence are noted below with a scheduled completion date of March 30, 2018.

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

The primary mitigation activity has already taken place, and the [REDACTED] has been [REDACTED]. This has mitigated this activity and reduced the risk to the BES. Add a review/escalation process to [REDACTED].

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

The successful completion of the Mitigation Plan will minimize the probability of this occurring again by formally add a [REDACTED] CIP-002 [REDACTED] to related [REDACTED] when changes in [REDACTED]. This will add clarity to all [REDACTED] of how much the [REDACTED] is [REDACTED], so the [REDACTED] will not [REDACTED] thereby reducing the risk to the BES. [REDACTED] has already moved the [REDACTED]. To further reduce the future risk to the BES system [REDACTED], further [REDACTED] enhancing the stability of the BES by [REDACTED] with [REDACTED] capabilities not found at the [REDACTED].

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements




Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

- \* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and
- \* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.
2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.
3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

 Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: \_\_\_\_\_  
(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: 

Title: 

Authorized On: January 03, 2018

### Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6)

Registered Entity Name: [REDACTED]

NERC Registry ID: [REDACTED]

NERC Violation ID(s): RFC2017018708

Mitigated Standard Requirement(s): CIP-002-5.1 R1.

Scheduled Completion as per Accepted Mitigation Plan: April 09, 2018

Date Mitigation Plan completed: April 02, 2018

RF Notified of Completion on Date: April 09, 2018

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[REDACTED]		28,705,251

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [REDACTED]

Title: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

## Mitigation Plan Verification for RFC2017018708

---

**Standard/Requirement:** CIP-002-5.1 R1

**NERC Mitigation Plan ID:** RFCMIT013479

**Method of Disposition:** Not yet determined

Relevant Dates					
Initiating Document	Mitigation Plan Submittal	RF Acceptance	NERC Approval	Certification Submittal	Date of Completion
Self-Report 11/21/17	01/03/18	01/29/18	02/15/18	04/09/18	3/19/18

### Description of Issue

[Mitigation Task RFC2017018708](#)

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	[REDACTED]	CIP-002-5.1 R1
File 2	Response Questions for [REDACTED] on RFC2017018708	CIP-002-5.1 R1
File 3	RFC2017018708 Certification Package	CIP-002-5.1 R1

### Verification of Mitigation Plan Completion

**Milestone 1:** [REDACTED]

Proposed Completion Date: November 14, 2017

Actual Completion Date: November 14, 2017

File 1, [REDACTED]", Pages 2 through 18, shows that the [REDACTED] of November 17, 2017. The [REDACTED] to the [REDACTED] [REDACTED] [REDACTED] This moves the [REDACTED] [REDACTED]

Milestone # 1 Completion verified.

**Milestone 2:** Add a review/escalation process to [REDACTED]

Proposed Completion Date: February 6, 2018

Actual Completion Date: March 19, 2018

File 3, "RFC2018019261 Certification Package", Milestone 2- Submit, Pages 5, show the escalation into CIP-002 scope via an email notification or call to the required program manager.

Milestone # 2 Completion verified.

**Milestone 3:** Add formal [REDACTED] in CIP-002 annual.

Proposed Completion Date: April 9, 2018

Actual Completion Date: March 19, 2018

File 3, "RFC2018019261 Certification Package", Milestone 3- Submit, Pages 2 through 47, show the past and updated [REDACTED] showing the new requirements into CIP-002 program such as the integration of the [REDACTED] to the entities' [REDACTED]. These procedures and defined checks ensure that [REDACTED]

Milestone # 3 Completion verified.

The Mitigation Plan is hereby verified complete.



NON-PUBLIC AND  
CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED  
FROM THIS PUBLIC VERSION

A handwritten signature in black ink, consisting of a stylized 'A' followed by a long horizontal line that curves upwards at the end.

Date: August 27, 2018

Anthony Jablonski  
Manager, Risk Analysis & Mitigation  
ReliabilityFirst Corporation

## Attachment 3

## Record documents for the violation of CIP-004-6 R2

- 3.a The Entity's Self-Report (RFC2017017778);
- 3.b The Entity's Mitigation Plan designated as RFCMIT012999 submitted [REDACTED];
- 3.c The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
- 3.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED]

Self Report

Entity Name: [REDACTED]

NERC ID: [REDACTED]

Standard: CIP-004-6

Requirement: CIP-004-6 R2.

Date Submitted: [REDACTED]

Has this violation previously No  
been reported or discovered?:

Entity Information:

Joint Registration  
Organization (JRO) ID:

Coordinated Functional  
Registration (CFR) ID:

Contact Name: [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: June 15, 2017 **Changed to April 12, 2017**

End/Expected End Date:

Reliability Functions: [REDACTED]

Is Possible Violation still No  
occurring?:

Number of Instances: 1

Has this Possible Violation No  
been reported to other  
Regions?:

Which Regions:

Date Reported to Regions:

Detailed Description and Detailed Description:  
Cause of Possible Violation:

[REDACTED]. In order for an individual to meet a [REDACTED]  
requirement, all the [REDACTED] associated with it must be met.  
[REDACTED]. [REDACTED].  
[REDACTED]  
[REDACTED]. [REDACTED]  
[REDACTED]  
[REDACTED].

[REDACTED] is provided to gain a better  
understanding of the basic information concerning NERC CIP training roles,  
Cyber Security Policy documents, Cyber Security Incidents and [REDACTED].  
Participants will also learn about the systems and  
controls in place to allow / restrict access to Physical Security Perimeters  
(PSPs), Physical Access Control System (PACS), and the [REDACTED]  
and [REDACTED].  
As noted in paragraph above both [REDACTED] AND [REDACTED] are  
required in order to obtain the [REDACTED]. However, on  
1/5/2017, the [REDACTED] changed the definition of [REDACTED].

Self Report

[REDACTED]

On 1/6/2017, the [REDACTED] was changed back to the [REDACTED] AND [REDACTED] With the [REDACTED] allowed [REDACTED] pers [REDACTED] before the correction. Out of [REDACTED] potential opportunities for access authorization error, only one employee was granted access.

On 4/12/17, an employee who had only [REDACTED] [REDACTED] requested access and [REDACTED] provided the [REDACTED] [REDACTED] because of the [REDACTED] [REDACTED] on 1/5/2017. On 5/8/17, after the identification of the potential noncompliance [REDACTED] immediately revoked this employee's access and also [REDACTED] on 5/9/2017. Door access logs indicate employee entered [REDACTED] on three separate occasions prior to access being revoked on 5/9/17.

Extent of condition using the true-up process identified that [REDACTED] employees only completed the [REDACTED] course but no access was granted. The supervisors of the [REDACTED] employees could have requested access to a Physical Security Perimeter, in this instance only one supervisor did and that employee entered a Physical Security Perimeter. This is a Possible Non-Compliance of NERC Standard CIP-004-6 R2.2.

The change on 1/5/2017 was initiated because the curriculum was changed from alignment to [REDACTED] NERC accesses in [REDACTED] in 2016, to alignment with high level [REDACTED] NERC roles in 2017. This forced us to combine content into fewer courses in the training program which made it easier for both the student to complete the courses and course completion tracking to ensure compliance with updated [REDACTED] NERC training requirements. In 2016, [REDACTED] [REDACTED] required three [REDACTED] [REDACTED] and in 2017 only required [REDACTED] [REDACTED] Super Qualification [REDACTED] name changed from [REDACTED] [REDACTED] in 2016 to [REDACTED] in 2017.

Root Cause of Possible Violation:

[REDACTED] [REDACTED] was erroneously changed in the [REDACTED] by a programmer who recently took on the task of updating the [REDACTED] The root cause was determined to be lack of job aid defining the rules that make up a [REDACTED] [REDACTED]

How was the violation discovered?

A [REDACTED] [REDACTED] between [REDACTED] databases was performed as scheduled. [REDACTED] discovered an employee had physical access to a NERC Protected asset without record or evidence of having completed the NERC Ops training-[REDACTED] [REDACTED]

Timeline:

1/5/2017- A [REDACTED] [REDACTED] changed the definition of [REDACTED] [REDACTED] so that either [REDACTED] [REDACTED] or [REDACTED] would grant the [REDACTED] [REDACTED] [REDACTED]  
1/6/2017- The [REDACTED] [REDACTED] changed the definition back to its [REDACTED], the definition was changed to its [REDACTED] [REDACTED] with updated [REDACTED] NERC training requirements. The correction of the [REDACTED] on 1/6/2017 did not reverse and correct the training status for affected [REDACTED] [REDACTED]  
4/12/2017- An employee was granted physical unescorted access through [REDACTED] without the employee having completed the required training for such access. The manager of the employee requested access through [REDACTED]. The employee was granted access because the incorrect [REDACTED] [REDACTED] was still in place after the coding error on 1/5/2017.  
5/8/2017- A [REDACTED] [REDACTED] between [REDACTED] databases was performed as scheduled. [REDACTED] discovered an employee had physical access to a NERC Protected Asset without record or evidence of having completed the [REDACTED] training. The [REDACTED] between [REDACTED] and [REDACTED]

Self Report

[REDACTED] was a [REDACTED].  
5/9/2017- Inactivation of [REDACTED] [REDACTED] to all [REDACTED] employees that were provided the [REDACTED] based on the [REDACTED]. The [REDACTED] does not contain the [REDACTED] that were granted [REDACTED].

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Mitigating Activities: Employee who had the physical access granted had an active PRA. The removal of [REDACTED] [REDACTED] from the [REDACTED] employees as well as unescorted physical access to the one employee who received it, brought us back into compliance with CIP-004-6 R2.2.

Preventive Measures:  
The [REDACTED] has since created a job aide for changing and creating [REDACTED]. In addition, a [REDACTED] to explain the [REDACTED] behind definitions will be created.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe  
Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: Potential: potential risk was severe due to [REDACTED], [REDACTED] employees could have been potentially granted unauthorized access.

Actual: actual risk minimal because of those [REDACTED] employees only one employee was granted unauthorized access

Risk Assessment of Impact to BPS: Everyone had a current PRA (Personnel Risk Assessment) conducted so the risk of them doing harm is low. They did not have the proper training to enter due to [REDACTED], but we did not give access to someone without conducting a background check.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

## Mitigation Plan

### Mitigation Plan Summary

Registered Entity: [REDACTED]

Mitigation Plan Code:

Mitigation Plan Version: 1

<u>NERC Violation ID</u>	<u>Requirement</u>	<u>Violation Validated On</u>
RFC2017017778	CIP-004-6 R2.	

Mitigation Plan Submitted On: [REDACTED]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: July 06, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [REDACTED] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

## Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

- (1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
  - (2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
  - (3) The cause of the Alleged or Confirmed Violation(s).
  - (4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
  - (5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
  - (6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
  - (7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
  - (8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
  - (9) Any other information deemed necessary or appropriate.
  - (10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
  - (11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.
- The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.
  - This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.
  - If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.
  - Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.
  - Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.
  - The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [REDACTED]

NERC Compliance Registry ID: [REDACTED]

Address: [REDACTED]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [REDACTED]

Title: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]



Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017017778	06/15/2017	CIP-004-6 R2.

Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

Brief Description: (What happened?)

[REDACTED]

[REDACTED] is provided to gain a better understanding of the basic information [REDACTED].

[REDACTED]. This consists of [REDACTED] and [REDACTED].

As noted in paragraph above both [REDACTED] AND [REDACTED] are required in order to obtain the [REDACTED]. However, on 1/5/2017, the [REDACTED] changed the definition of [REDACTED] to [REDACTED] OR [REDACTED].

On 1/6/2017, the [REDACTED] was changed back to the correct [REDACTED] AND [REDACTED]. With the [REDACTED], the system allowed [REDACTED] personnel with either [REDACTED] to be granted the [REDACTED] before the correction. Out of [REDACTED] potential opportunities for access authorization error, only one employee was granted access.

On 4/12/17, an employee who had only [REDACTED] requested access and [REDACTED] provided the [REDACTED] [REDACTED] because of the incorrect status set on 1/5/2017. On 5/8/17, after the identification of the potential noncompliance [REDACTED] immediately revoked this employee's access and also [REDACTED] on 5/9/2017. Door access logs indicate employee entered [REDACTED] on three separate occasions prior to access being revoked on 5/9/17.

Extent of condition using the [REDACTED] identified that [REDACTED] employees only completed the [REDACTED] course but no access was granted. The supervisors of the [REDACTED] employees could have requested access to a Physical Security Perimeter, in this instance only one supervisor did and that employee entered a Physical Security Perimeter. This is a Possible Non-Compliance of NERC Standard CIP-004-6 R2 P2.2. The change on 1/5/2017 was initiated because the [REDACTED] to [REDACTED] NERC accesses in [REDACTED] in 2016, to alignment with high level [REDACTED] NERC roles in 2017. This forced us to combine [REDACTED] into [REDACTED].

[REDACTED] NERC training requirements. In 2016, [REDACTED] required three [REDACTED] and [REDACTED] and in 2017 only required [REDACTED] [REDACTED] name changed from [REDACTED] in 2016 to NERC Operations in 2017.

Cause: (what caused the violation?)

[REDACTED] was erroneously changed in the [REDACTED] [REDACTED] by a programmer who recently took on the task of updating the [REDACTED].

Results of the RCA: (What is the root cause?)

The root cause was determined to be lack of job aid defining the rules that make up a [REDACTED].

Relevant information regarding the identification of the violation(s):

A [REDACTED] between [REDACTED] and [REDACTED] databases was performed as scheduled. [REDACTED] discovered an employee had physical access to a NERC Protected asset without record or evidence of having completed the NERC Ops training- [REDACTED] [REDACTED]

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

Milestone 1- Inactivate [REDACTED] for all [REDACTED] employees as well as physical access removal from one employee. The inactivation of the [REDACTED] and the physical access removal from the employee who entered the PSP on 3 separate occasions brought us back into compliance with CIP-004-6 R2. P2.2. A report has been generated to support that all [REDACTED] employees had [REDACTED] revoked.  
 Milestone 2- Ensure the process for changing and creating a [REDACTED] is documented and requires an independent verification of changes. This error occurred in part, due to a lack of job aides existing to ensure a [REDACTED] understood the process behind changing and creating [REDACTED]. A job aide has since been created, it will provide clear and concise instructions to [REDACTED] performing such changes, [REDACTED].

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: July 06, 2017

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
1. Inactivation of the [REDACTED] and physical access removal	Revoke the [REDACTED] for [REDACTED] employees who received it due to a [REDACTED]	05/09/2017	05/09/2017		No
2. Process for changing and creating a [REDACTED] is documented and requires an independent verification of changes	A process did not exist prior to this occurrence. The job aide will provide instructions to [REDACTED] to ensure changes/additions to [REDACTED] meet programming and [REDACTED] of [REDACTED]. The independent review will serve as an additional control to ensure changes to [REDACTED]	07/06/2017			No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
	[REDACTED] [REDACTED] are correct.				

Additional Relevant Information

## Reliability Risk

### Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

██████ has not identified any additional risk to the BES. Everyone had a current Personnel Risk Assessment (PRA) conducted so the risk of them doing harm is low. They did not have the proper training to enter due to coding error, but we did not give access to someone without conducting a PRA.

### Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

In order to address future BES reliability risk ██████ has taken several steps to both address the violation identified in this mitigation plan and to prevent possible reoccurrences of this violation. The removal of ██████ to all ██████ employees and removal of physical access to one employee brought ██████ back into a compliant state with CIP-004-6 R2. P2.2. In addition, a job aide has been created for ██████ to follow when creating and changing ██████ that includes an independent review of the changes. This will ensure changes/creations of ██████ are valid and meet the programming and ██████ of ██████

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

---

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

- \* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and
- \* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.
2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.
3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

██████████ Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: \_\_\_\_\_

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: ██████ ██████

Title: ██

Authorized On: ████████████████

### Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6)

Registered Entity Name: [REDACTED]

NERC Registry ID: [REDACTED]

NERC Violation ID(s): RFC2017017778

Mitigated Standard Requirement(s): CIP-004-6 R2.

Scheduled Completion as per Accepted Mitigation Plan: [REDACTED]

Date Mitigation Plan completed: [REDACTED]

RF Notified of Completion on Date: [REDACTED]

Entity Comment: Supporting Certification Evidence Package uploaded in Entity Documents as RFC2017017778.zip

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017778 Certification.zip	The file "RFC2017017778 Certification.zip" contains:  RFC2017017778 Certification cover page.pdf - cover page for overall package.  Milestone 1 - Submit.pdf - evidence supporting milestone Milestone 2 - Submit.pdf - evidence supporting milestone	20,371,711

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [REDACTED]

Title: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

## Mitigation Plan Verification for RFC2017017778

---

[REDACTED]

**Standard/Requirement:** CIP-004-6 R2

**NERC Mitigation Plan ID:** RFCMIT012999

**Method of Disposition:** Not yet determined

Relevant Dates					
Initiating Document	Mitigation Plan Submittal	RF Acceptance	NERC Approval	Certification Submittal	Date of Completion
Self-Report [REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]

### Description of Issue

[REDACTED]

[REDACTED]

[REDACTED]. Door access logs indicate employee entered [REDACTED] on three separate occasions prior to access being revoked on 5/9/17.

Extent of condition using the [REDACTED] process identified that [REDACTED] employees only completed the IM (Information Management) course but no access was granted. The supervisors of the [REDACTED] employees could have requested access to a Physical Security Perimeter, in this instance only one



supervisor did and that employee entered a Physical Security Perimeter. This is a Possible Non-Compliance of NERC Standard CIP-004-6 R2 P2.2.

The root cause was determined to be lack of job aid defining the rules that make up a super qualification.

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	RFC2017017778 Certification	CIP-004-6 R2

### Verification of Mitigation Plan Completion

**Milestone 1:** Inactivation of the [REDACTED] and physical access removal.

File 1, “RFC2017017778 Certification”, RFC2017017778 Milestone 1-200 as evidence of a Completed Request that documents the physical access removal of the one employee who was granted access.

File 1, “RFC2017017778 Certification”, RFC2017017778 Milestone 1-100 as evidence shows that the [REDACTED] employees who had [REDACTED] [REDACTED] were removed.

Milestone # 1 Completion verified.

**Milestone 2:** Process for changing and creating a Super Qualification is documented and requires an independent verification of changes.

File 1, “RFC2017017778 Certification”, RFC2017017778 Milestone 2-100 as evidence of the process map that reflects the independent review of the changes to adding or changing of qualifications.

File 1, “RFC2017017778 Certification”, RFC2017017778 Milestone 2-200 as evidence of a Standard Work Instruction that guides qualification managers through the process of defining or editing a [REDACTED] [REDACTED].

Milestone # 2 Completion verified.

NON-PUBLIC AND  
CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED  
FROM THIS PUBLIC VERSION

The Mitigation Plan is hereby verified complete.

A handwritten signature in black ink that reads "Tony Purgar". The signature is fluid and cursive, with the first name "Tony" and last name "Purgar" clearly legible.

Date: [REDACTED]

Tony Purgar  
Manager, Risk Analysis & Mitigation  
ReliabilityFirst Corporation