

January 25, 2019

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]
[REDACTED]
FERC Docket No. NP19-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty regarding [REDACTED] with information and details regarding the nature and resolution of the violations² discussed in detail in the Settlement Agreement attached hereto (Attachment A), 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)).³

NERC is filing this Notice of Penalty with the Commission because [REDACTED]

² 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.

³ See 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

NERC Notice of Penalty

The Companies

January 25, 2019

Page 2

(collectively, the Regional Entities (REs)) and the Companies have entered into a Settlement Agreement to resolve all outstanding issues arising from the REs' determination and findings of 127 violations of the Critical Infrastructure Protection (CIP) NERC Reliability Standards.

According to the Settlement Agreement, the Companies agree to the assessed penalty of ten million dollars (\$10,000,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

For the reasons discussed below, NERC is providing public and non-public versions of this filing pursuant to Sections 39.7(b)(4) and 388.113 of the Commission's regulations. In the public version of this filing, NERC redacted sensitive information that qualifies for non-public treatment under Sections 39.7(b)(4) or 388.113. NERC respectfully requests that the Commission designate the redacted portions of the filing as non-public and as Critical Energy/Electric Infrastructure Information (CEII), consistent with Sections 39.7(b)(4) and 388.113.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between the REs and the Companies. 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 (2017), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement and herein.

| NERC Violation ID | Standard | Req. | VRF/ VSL | Applicable Function(s) | Discovery Method* | Risk |
|-------------------|-------------|------|----------------|------------------------|-------------------|----------|
| [REDACTED] | CIP-002-5.1 | R1.2 | High/ Lower | [REDACTED] | SR | Moderate |
| [REDACTED] | CIP-002-5.1 | R1.2 | High/ Lower | [REDACTED] | SR | Minimal |
| [REDACTED] | CIP-002-5.1 | R1.2 | High/ Lower | [REDACTED] | SR | Minimal |
| [REDACTED] | CIP-002-5.1 | R1.2 | High/ Lower | [REDACTED] | SR | Minimal |

NERC Notice of Penalty
The Companies
January 25, 2019
Page 3

| NERC Violation ID | Standard | Req. | VER/ VSL | Applicable Function(s) | Discovery Method* | Risk |
|-------------------|------------|--------------|--------------------|------------------------|-------------------|----------|
| | CIP-003-3 | R4.2 | Lower/ Severe | | SR | Moderate |
| | CIP-003-3 | R6 | Lower/ Severe | | CA | Moderate |
| | CIP-003-3 | R6 | Lower/ Severe | | SR | Moderate |
| | CIP-003-3 | R6 | Lower/ Severe | | SR | Moderate |
| | CIP-003-3 | R6 | Lower/ Severe | | SR | Minimal |
| | CIP-004-3a | R2.1 | Lower/ Severe | | SR | Moderate |
| | CIP-004-6 | R2; P2.2 | Lower/ Lower | | SR | Minimal |
| | CIP-004-6 | R2; P2.3 | Lower/ Lower | | SR | Moderate |
| | CIP-004-3a | R3.2 | Lower/ Moderate | | SR | Minimal |
| | CIP-004-6 | R3; P3.5 | Medium/ Lower | | SR | Minimal |
| | CIP-004-6 | R3; P3.5 | Medium/ Lower | | SR | Moderate |
| | CIP-004-3a | R4.2 | Lower/ Severe | | CA | Minimal |
| | CIP-004-3a | R4.2 | Lower/ Severe | | SR | Minimal |
| | CIP-004-3a | R4.2 | Lower/ Severe | | SR | Minimal |
| | CIP-004-6 | R4; P4.1 | Medium/ Severe | | SR | Moderate |
| | CIP-004-6 | R4; P4.1 | Medium/ Severe | | SR | Minimal |
| | CIP-004-6 | R4; P4.1 | Medium/ Severe | | SR | Minimal |
| | CIP-004-6 | R4; P4.1 | Medium/ Severe | | SR | Moderate |
| | CIP-004-6 | R4; P4.2, | Medium/ Severe | | SR | Minimal |

NERC Notice of Penalty
The Companies
January 25, 2019
Page 4

| NERC Violation ID | Standard | Req. | VRF/ VSL | Applicable Function(s) | Discovery Method* | Risk |
|-------------------|------------|-------------------------------|---------------------|------------------------|-------------------|----------|
| | | P4.3, P4.4 | | | | |
| | CIP-004-6 | R5; P5.1 | Medium/ Moderate | | SR | Moderate |
| | CIP-004-6 | R5; P5.1 | Medium/ Moderate | | SR | Moderate |
| | CIP-004-6 | R5; P5.2 | Medium/ Moderate | | SR | Minimal |
| | CIP-004-6 | R5; P5.2 | Medium/ Moderate | | SR | Minimal |
| | CIP-004-6 | R5; P5.2 | Medium/ Moderate | | SR | Moderate |
| | CIP-004-6 | R5; P5.2 | Medium/ Moderate | | SR | Minimal |
| | CIP-004-6 | R5; P5.2, P5.3, P5.4 | Medium/ Moderate | | SR | Moderate |
| | CIP-005-1 | R1.4 | Medium/ Severe | | SR | Moderate |
| | CIP-005-3a | R1.4 | Medium/ Severe | | SR | Minimal |
| | CIP-005-3a | R1.4 | Medium/ Severe | | SR | Minimal |
| | CIP-005-3a | R1.5 | Medium/ Severe | | SR | Moderate |
| | CIP-005-3a | R1.5 | Medium/ Severe | | SR | Minimal |
| | CIP-005-3a | R1.5 | Medium/ Severe | | SR | Moderate |
| | CIP-005-5 | R1; P1.3 | Medium/ Severe | | CA | Moderate |
| | CIP-005-5 | R1; P1.3 | Medium/ Severe | | SR | Moderate |
| | CIP-005-5 | R1; P1.3 | Medium/ Severe | | SR | Serious |
| | CIP-005-5 | R1; P1.5 | Medium/ Severe | | SR | Moderate |

NERC Notice of Penalty
The Companies
January 25, 2019
Page 5

| NERC Violation ID | Standard | Req. | VRF/ VSL | Applicable Function(s) | Discovery Method* | Risk |
|-------------------|------------|-------------------------------|-------------------|------------------------|-------------------|----------|
| | CIP-005-3a | R2.1, R2.2, R2.4 | Medium/ High | | SR | Serious |
| | CIP-005-3a | R2.2 | Medium/ High | | SR | Minimal |
| | CIP-005-3a | R2.5.3 | Medium/ High | | SR | Moderate |
| | CIP-005-5 | R2; P2.1 | Medium/ High | | SR | Moderate |
| | CIP-005-5 | R2; P2.1 | Medium/ High | | SR | Moderate |
| | CIP-005-5 | R2; P2.1 | Medium/ High | | SR | Minimal |
| | CIP-005-5 | R2; P2.1, P2.2, P2.3 | Medium/ High | | CA | Moderate |
| | CIP-005-5 | R2; P2.1, P2.2, P2.3 | Medium/ High | | SR | Minimal |
| | CIP-006-3c | R1.1 | Medium/ Severe | | SR | Minimal |
| | CIP-006-3c | R1.5 | Medium/ Severe | | SR | Minimal |
| | CIP-006-3c | R1.6 | Medium/ Severe | | SR | Serious |
| | CIP-006-3c | R1.6.2 | Medium/ Severe | | SR | Minimal |
| | CIP-006-6 | R1; P1.1 | Medium/ Severe | | SR | Minimal |
| | CIP-006-6 | R1; P1.2 | Medium/ Severe | | SR | Serious |
| | CIP-006-6 | R1; P1.4 | Medium/ Severe | | SR | Minimal |
| | CIP-006-6 | R1; P1.8 | Medium/ Severe | | SR | Minimal |

NERC Notice of Penalty
The Companies
January 25, 2019
Page 6

| NERC Violation ID | Standard | Req. | VER/ VSL | Applicable Function(s) | Discovery Method* | Risk |
|-------------------|------------|------------------------|-------------------|------------------------|-------------------|----------|
| | CIP-006-3c | R2.2 | Medium/ Severe | | SR | Minimal |
| | CIP-006-3c | R2.2 | Medium/ Severe | | SR | Minimal |
| | CIP-006-6 | R2; P2.1 | Medium/ Severe | | SR | Minimal |
| | CIP-006-6 | R2; P2.2 | Medium/ Severe | | SR | Minimal |
| | CIP-006-6 | R2; P2.2 | Medium/ Severe | | CA | Minimal |
| | CIP-006-6 | R2; P2.2 | Medium/ Severe | | SR | Minimal |
| | CIP-006-6 | R2; P2.2 | Medium/ Severe | | SR | Minimal |
| | CIP-006-6 | R2; P2.2 | Medium/ Severe | | SR | Minimal |
| | CIP-006-6 | R2; P2.2 | Medium/ Severe | | SR | Minimal |
| | CIP-006-6 | R2; P2.2 | Medium/ Severe | | SR | Minimal |
| | CIP-006-3c | R4 | Medium/ Severe | | SR | Moderate |
| | CIP-006-3c | R5 | Medium/ Severe | | SR | Moderate |
| | CIP-006-3c | R5 | Medium/ Severe | | SR | Minimal |
| | CIP-006-3c | R5 | Medium/ Severe | | SR | Moderate |
| | CIP-006-3c | R5 | Medium/ Severe | | SR | Moderate |
| | CIP-006-3c | R5 | Medium/ Severe | | SR | Serious |
| | CIP-007-3a | R1.1, R1.2, R1.3 | Medium/ Severe | | CA | Moderate |
| | CIP-007-3a | R1.1 | Medium/ Severe | | SR | Serious |

NERC Notice of Penalty
The Companies
January 25, 2019
Page 7

| NERC Violation ID | Standard | Req. | VRF/ VSL | Applicable Function(s) | Discovery Method* | Risk |
|-------------------|------------|--|---------------------|------------------------|-------------------|----------|
| | CIP-007-3a | R1.1 | Medium/ Severe | | SR | Moderate |
| | CIP-007-6 | R1; P1.1 | Medium/ High | | SR | Moderate |
| | CIP-007-6 | R2; P2.2 | Medium/ High | | SR | Moderate |
| | CIP-007-6 | R2; P2.2 | Medium/ High | | SR | Moderate |
| | CIP-007-6 | R2; P2.2 | Medium/ High | | SR | Moderate |
| | CIP-007-6 | R2; P2.2 | Medium/ High | | SR | Moderate |
| | CIP-007-6 | R2; P2.3 | Medium/ High | | SR | Moderate |
| | CIP-007-3a | R3.1 | Lower/ Severe | | SR | Moderate |
| | CIP-007-3a | R3 | Lower/ Severe | | SR | Serious |
| | CIP-007-6 | R3; P3.3 | Medium/ Moderate | | SR | Moderate |
| | CIP-007-6 | R4; P4.1, P4.2, P4.3, P4.4 | Medium/ Severe | | SR | Serious |
| | CIP-007-6 | R4; P4.4 | Medium/ Severe | | CA | Moderate |
| | CIP-007-3a | R5.1 | Lower/ Severe | | SR | Moderate |
| | CIP-007-3a | R5.2 | Lower/ Severe | | SR | Minimal |
| | CIP-007-3a | R5.3 | Lower/ Severe | | SR | Moderate |
| | CIP-007-3a | R5.2, R5.3 | Lower/ Severe | | SR | Serious |
| | CIP-007-6 | R5; P5.1, P5.2, | Medium/ Severe | | SR | Moderate |

NERC Notice of Penalty
The Companies
January 25, 2019
Page 8

| NERC Violation ID | Standard | Req. | VRF/ VSL | Applicable Function(s) | Discovery Method* | Risk |
|-------------------|------------|---|-------------------|------------------------|-------------------|----------|
| | | P5.3, P5.4, P5.5, P5.6, P5.7 | | | | |
| | CIP-007-6 | R5; P5.2 | Medium/ Severe | | SR | Serious |
| | CIP-007-6 | R5; P5.6 | Medium/ Severe | | SR | Moderate |
| | CIP-007-3a | R6.2 | Lower/ Severe | | CA | Moderate |
| | CIP-007-3a | R7.1 | Lower/ Severe | | SR | Minimal |
| | CIP-007-3a | R8.4 | Lower/ Severe | | SR | Moderate |
| | CIP-007-3a | R9 | Lower/ High | | SR | Minimal |
| | CIP-009-6 | R1; P1.1, P1.2, P1.3, P1.4, P1.5 | Medium/ Severe | | SR | Moderate |
| | CIP-009-6 | R2; P2.1, P2.2 | Lower/ Severe | | SR | Moderate |
| | CIP-009-6 | R3; P3.1, P3.1.1, P3.1.2, P3.1.3, P3.2, P3.2.1, P3.2.2 | Lower/ Severe | | SR | Moderate |
| | CIP-010-2 | R1; P1.1 | Medium/ Severe | | CA | Minimal |
| | CIP-010-2 | R1; P1.1.1 | Medium/ Severe | | SR | Minimal |

NERC Notice of Penalty
The Companies
January 25, 2018
Page 9

| NERC Violation ID | Standard | Req. | VRV/ VSL | Applicable Function(s) | Discovery Method* | Risk |
|-------------------|-----------|-----------------------------------|-------------------|------------------------|-------------------|----------|
| | CIP-010-2 | R1; P1.1, P1.1.1, P1.1.4 | Medium/ Severe | | SR | Serious |
| | CIP-010-2 | R1; P1.1.4 | Medium/ Severe | | SR | Moderate |
| | CIP-010-2 | R1; P1.1.4 | Medium/ Severe | | CA | Moderate |
| | CIP-010-2 | R1; P1.1.4 | Medium/ Severe | | SR | Minimal |
| | CIP-010-2 | R1; P1.1.5 | Medium/ Severe | | SR | Moderate |
| | CIP-010-2 | R1; P1.2 | Medium/ Severe | | SR | Minimal |
| | CIP-010-2 | R1; P1.2 | Medium/ Severe | | SR | Minimal |
| | CIP-010-2 | R1; P1.2 | Medium/ Severe | | SR | Minimal |
| | CIP-010-2 | R1; P1.4.1, P1.4.2 | Medium/ Severe | | CA | Minimal |
| | CIP-010-2 | R1; P1.4.1, P1.4.2 | Medium/ Severe | | SR | Moderate |
| | CIP-010-2 | R2; P2.1 | Medium/ Severe | | CA | Moderate |
| | CIP-010-2 | R2; P2.1 | Medium/ Severe | | SR | Minimal |
| | CIP-010-2 | R2; P2.1 | Medium/ Severe | | SR | Minimal |
| | CIP-010-2 | R2; P2.1 | Medium/ Severe | | SR | Moderate |
| | CIP-010-2 | R3; P3.3 | Medium/ Severe | | SR | Moderate |
| | CIP-010-2 | R3; P3.3 | Medium/ Severe | | CA | Moderate |

NERC Notice of Penalty
The Companies
January 25, 2018
Page 10

| NERC Violation ID | Standard | Req. | VRF/ VSL | Applicable Function(s) | Discovery Method* | Risk |
|-------------------|-----------|------------------------------|-------------------|------------------------|-------------------|----------|
| | CIP-010-2 | R3; P3.1, P3.3 P3.4 | Medium/ Severe | | SR | Moderate |
| | CIP-010-2 | R4 | Medium/ Severe | | SR | Serious |
| | CIP-010-2 | R4 | Medium/ Severe | | SR | Minimal |
| | CIP-011-2 | R1; P1.2 | Medium/ Severe | | SR | Moderate |
| | CIP-011-2 | R1; P1.2 | Medium/ Severe | | SR | Moderate |
| | CIP-011-2 | R1; P1.2 | Medium/ Severe | | SR | Serious |
| | CIP-011-2 | R1; P1.1, P1.2 | Medium/ Severe | | SR | Moderate |
| | CIP-011-2 | R2; P2.1, P.2.2 | Lower/ Severe | | SR | Moderate |
| | CIP-014-2 | R1 | High/ Severe | | SR | Moderate |

FACTS COMMON TO VIOLATIONS

These violations were discovered during CIP Compliance Audits and through Self-Reports the Companies submitted from 2015 through 2018.

These issues displayed the following contributing causes:

- Lack of management engagement, support, and accountability relating to the CIP compliance program;
- Disassociation of compliance and security that resulted in a deficient program and program documents, lack of implementation, and ineffective oversight and training;

NERC Notice of Penalty

The Companies

January 25, 2019

Page 11

- Organizational silos in the form of a lack of communication between management levels within the Companies, which contributed to a lack of awareness of the state of security and compliance; and
- Organizational silos across business units that resulted in confusion regarding expectations and ownership of tasks, and poor asset and configuration management practices.

To address these causes, the Companies committed to additional measures, apart from mitigation activities, to help ensure the effectiveness and sustainability of the CIP compliance and security program. These activities include:

- Increasing senior leadership involvement and oversight;
- Creating a centralized CIP oversight department and restructuring roles within that department to focus on areas such as Standards, Enterprise Oversight, Enterprise CIP Tools, compliance metrics, and regulatory interactions;
- Conducting industry surveys and benchmark discussions to help develop best practices relating to sustainable security and compliance practices; and
- Continuing to develop an in-house CIP program and talent development program.

Similarly, the Companies committed to implement measures to support and assist staff in implementing a sustainable CIP compliance program. These activities include:

- Investing in enterprise-wide tools relating to asset and configuration management, visitor logging, access management, and configuration monitoring and vulnerability assessments;
- Adding resources to help manage and implement compliance and security efforts;
- Instituting annual compliance drills; and
- Creating three levels of training (oversight training, awareness training for all staff, and performance training for staff implementing the security and compliance tasks).

The Companies have engaged with the REs during the enforcement process for the purpose of comprehensively evaluating and improving the Companies' overall security posture. This allowed the Companies to gain an objective and more accurate understanding of their compliance program and security posture, as well as the changes necessary to address the underlying issues in order to implement an effective and sustainable CIP program. In addition to focusing on the cultural and enterprise-wide changes necessary to establish a solid foundation for a sustainable CIP program, the Companies are focusing on key risk areas, including patching, identifying deficiencies, and strategies for continuously improving the Companies' security posture and program sustainability.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 12

Due to the systemic nature of the violations, the causes contributing to the violations, the institution of enhanced programs and internal controls, and the Companies' shifting culture, the REs anticipate and expect that the Companies will identify additional instances of noncompliance as they complete mitigation and afterward, as they continue to mature their CIP program. The Companies' comprehensive mitigation and their sanctions (which are discussed below) require the Companies to promptly inform the REs of any compliance issues that the Companies identify. Upon notification of compliance issues, the REs will verify that an adequate root cause analysis is performed, the instances are timely mitigated, and the Companies continue the maturation of the CIP program.

RISK COMMON TO THE VIOLATIONS

The REs determined that, although the risk posed to the reliability of the bulk power system (BPS) by the individual violations ranged from minimal to serious (52 minimal, 62 moderate, and 13 serious), the 127 violations collectively posed a serious risk to the security and reliability of the BPS. The Companies' violations of the CIP Reliability Standards posed a higher risk to the reliability of the BPS because many of the violations involved long durations, multiple instances of noncompliance, and repeated failures to implement physical and cyber security protections. As an example, the Companies' failure to accurately document and track changes that deviate from existing baseline configurations increased the risk that the Companies would not identify unauthorized changes, which could adversely impact BES Cyber Systems (BCSs).

MITIGATION COMMON TO THE VIOLATIONS

The Companies submitted their mitigation activities to address the referenced violations (except for the violation of CIP-014-2) on September 11, 2018, included as Attachment 2. The Companies committed to taking the following actions by [REDACTED]

1. Revise their overarching corporate IT program to ensure that the program meets the requirements of all stakeholders and the CIP Standards;
2. Each of the Companies' business units will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the IT program;
3. Each business unit will conduct training on new and/or revised processes and procedures;
4. Each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and

NERC Notice of Penalty
The Companies
January 25, 2019
Page 13

5. The Companies will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document.

CIP-002-5.1a R1

1. The REs determined that [REDACTED] located in different [REDACTED] were not identified in the Companies' BES Cyber System (BCS) inventory.

The violation started when the Standard became mandatory and enforceable and ended when the Companies revised their BCS inventory to include the [REDACTED] for approximately 17 months of noncompliance.

2. The REs determined that the Companies had not identified [REDACTED] medium impact BCS and [REDACTED] associated BES Cyber Assets (BCAs) within a [REDACTED]

The violation started when the Companies failed to identify the BCS and associated BCAs that comprised the BCS and ended when the Companies revised their BCS inventory to include the associated BCAs, for approximately three months of noncompliance.

3. The REs determined that the Companies had not identified [REDACTED] in the BCS inventory.

The violation began when the Companies commissioned the [REDACTED] without identifying the [REDACTED] as BCAs and ended when the Companies updated their BCS inventory to include the [REDACTED] for approximately one month of noncompliance.

4. The REs determined that the Companies' BCA inventory list included an outdated cranking path associated with a Blackstart Resource.

The violation started when the Standard became mandatory and enforceable and ended when the Companies updated their BCS inventory to reflect the change in the correct cranking path, for approximately three months of noncompliance.

The primary cause of the violations was managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate moderate risk to the reliability of the BPS.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 14
CIP-003-3 R4

The REs determined that the Companies failed to protect Critical Cyber Asset (CCA) information in accordance with the Companies' information protection program, in two separate instances. In the first instance, the REs determined that [REDACTED] one-line diagrams did not have the appropriate NERC CIP classification markings. In the second instance, the REs determined that [REDACTED] of the Companies' employees were improperly granted "read-only" access rights to CCA information maintained in an information file repository.

The violation started when the Companies failed to mark CCA information and ended when the Companies modified the access permissions, thereby effectively revoking access rights to CCA information for unauthorized personnel, for approximately 51 months of noncompliance.

The violation involved insufficient training and a deficient process. Additional training was necessary to ensure that applicable IT personnel were aware that the file share contained sensitive CIP information that must be protected.

The REs determined that the violation posed a moderate risk to the reliability of the BPS.

CIP-003-3 R6

1. The REs determined that the Companies failed to follow their documented change control and configuration management process, in three instances. In all three instances, software upgrades were deployed on a single CCA in the production environment without first being tested in accordance with the Companies' change control process.

The violation started when, in the first instance, the software update was deployed without adherence to the Companies' change control and configuration management process and ended when the Companies conducted a vulnerability assessment and confirmed that the implementation of the service pack did not impact security controls, for approximately 35 months of noncompliance.

2. The REs determined that the Companies failed to adhere to their change control and configuration management process, in four instances. In the first instance, the Companies' employee installed a service pack on a [REDACTED] CCA. The service pack had not been tested prior to implementation in the production environment because it was not included as part of the authorized change request. In the second instance, the Companies' employee installed software on [REDACTED] non-CCA without an authorized change request. In the third instance, the Companies' employee failed to mark [REDACTED] Cyber Assets as NERC CIP assets prior to implementing

NERC Notice of Penalty
The Companies
January 25, 2019
Page 15

a software change. As a result, the software was not tested prior to implementation. In the fourth instance, the Companies' employee implemented an anti-virus software upgrade to [REDACTED] BCAs. The Companies' employee implemented an additional software upgrade on one CCA, which was not included in the authorized change request.

The violation started when, in the first instance, the software update was deployed without adherence to the Companies' change control and configuration management process and ended when the Companies' completed testing for the last instance, for approximately 11 weeks of noncompliance.

3. The REs determined that the Companies performed Distributed Control System upgrades on [REDACTED] but failed to maintain the necessary documentation throughout the change control and configuration management process.

The violation started when the Companies implemented a service pack on a CCA in the production environment without first testing it and ended when the Companies conducted a vulnerability assessment and confirmed that the implementation of the service pack did not impact security controls, for approximately 23 months of noncompliance.

4. The REs determined that the Companies replaced a failed [REDACTED] at a [REDACTED] [REDACTED] but did not update the asset database as required by the documented change control and configuration management process.

The violation started when the Companies replaced a [REDACTED] without updating the asset database and ended when the Companies updated the asset database and verified [REDACTED] baseline parameters, for approximately 17 months of noncompliance.

The primary cause of the CIP-003-3 R6 violations was lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-004-3a R2

The REs determined that the Companies failed to maintain annual cyber security training for [REDACTED] employees with authorized electronic access and/or physical access to CCAs.

NERC Notice of Penalty

The Companies

January 25, 2019

Page 16

The REs determined that the primary cause of the violation was lack of managerial oversight. The contributing causes were ineffective access management software, a deficient process, and lack of internal controls.

The violation started when the first individual's training expired and ended the last date that the Companies revoked access rights of the individuals whose training expired, for approximately two months of noncompliance.

The REs determined that the violation posed a moderate risk to the reliability of the BPS.

CIP-004-6 R2

1. The REs determined that the Companies did not provide cyber security training to an individual prior to granting electronic access to protected CAs.

The violation started on when the Companies granted electronic access to the passwords prior to training and ended when the Companies revoked the individual's access rights, for approximately 13 months of noncompliance.

2. The REs determined that the Companies failed to maintain training for one employee with access to applicable CAs.

The violation started when the individual's training expired and ended when the Companies revoked the individual's access rights, for approximately seven months of noncompliance.

The REs determined that the primary cause of the CIP-004-6 R2 violations was lack of managerial oversight. The contributing causes were a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate moderate risk to the reliability of the BPS.

CIP-004-3a R3

The REs determined that the Companies failed to timely update three employees' Personnel Risk Assessments (PRAs).

The REs determined that the primary cause was lack of managerial oversight. The contributing causes were a deficient process and weak internal controls.

NERC Notice of Penalty

The Companies

January 25, 2019

Page 17

The violation started the date the earliest PRA expired and ended the date the last PRA was renewed, for approximately nine months of noncompliance.

The REs determined that the violation posed a minimal risk to the BPS.

CIP-004-6 R3

1. The REs determined that the Companies failed to timely update a PRA for one contractor with unescorted physical access to BES Cyber Systems (BCSs).

The violation started the day following the expiration of the PRA and ended when the Companies revoked the contractor's physical access rights, for approximately five days of noncompliance.

2. The REs determined that the Companies failed to ensure individuals with authorized electronic and/or physical access to BCSs had current PRAs, in three instances. In the first instance, the Companies' [REDACTED] project team deviated from the processes for monitoring and revoking individuals' access rights, resulting in two employees with expired PRAs having access to [REDACTED] BCAs. In the second instance, the Companies failed to ensure that all individuals with authorized electronic and unescorted physical access to the Electronic Access Control and Monitoring Systems (EACMSs) had a current PRA. In the third instance, the Companies did not identify [REDACTED] servers as EACMSs. As a result, the Companies failed to ensure that all individuals with authorized electronic and unescorted physical access to the EACMS servers had a current PRA.

The violation started when, in the second and third instances, the Standard became mandatory and enforceable, and is currently ongoing.

The REs determined the primary cause of the CIP-004-6 R3 violations was lack of managerial oversight. The contributing causes were a deficient process, inadequate training, and lack of internal controls.

The REs determined the violations posed an aggregate moderate risk to the reliability of the BPS.

CIP-004-3a R4

1. The REs determined that the Companies failed to timely revoke a former employee's electronic access rights, in five instances. In the first instance, the Companies terminated the employee, but the Companies' manager did not notify the help desk per internal processes so that the help desk could immediately revoke access. In the second instance, the Companies'

NERC Notice of Penalty
The Companies
January 25, 2019
Page 18

contractor's employment ended, but the account manager did not follow the Companies' internal process of notifying the appropriate personnel to revoke the contractor's physical badge access to CCAs within seven calendar days from the date of termination. In the third instance, the Companies required a contractor to go on a 30-day absence, but the contractor's manager failed to follow the Companies' internal process of completing the required change access request documentation to revoke the contractor's physical badge access. In the fourth instance, the Companies failed to revoke access within seven calendar days for an employee who no longer required access to CCAs. In the fifth instance, the Companies failed to remove access for an employee because the badge access system was not designed to process NERC and non-NERC access requests or revocations on the same ticket.

The violation started when, in the first instance, the former employee's access rights were required to be revoked and ended when, in the fourth instance, the Companies revoked access, for approximately 10 months of noncompliance.

2. The REs determined that the Companies failed to revoke employees' access within seven calendar days after access was no longer required, in three instances. In the first instance, the Companies' manager initiated an access revocation, which was not finalized because the manager inadvertently kept the request in draft form. In the second instance, the Companies did not timely revoke employees' access rights that were no longer needed. In the third instance, the Companies failed to timely revoke two employees' authorized unescorted physical access to CCAs.

The violation started when one of the employee's access rights were required to be revoked and ended when, in the third instance, the Companies revoked the final employee's access rights, for approximately five months of noncompliance.

3. The REs determined that the Companies did not revoke a contractor's physical access rights within seven calendar days from the date of termination. The contractor changed employers, but the contractor's employer did not notify the Companies.

The violation started when the Companies should have revoked the former contractor's physical access rights and ended when the Companies revoked the physical access rights, for approximately 21 months of noncompliance.

The REs determined the primary cause was lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate moderate risk to the reliability of the BPS.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 19
CIP-004-6 R4

1. The REs determined that the Companies unnecessarily granted one individual unescorted physical access.

The violation started when the Companies granted the employee unnecessary access permissions to the PACSs and ended when the Companies removed the employee's access permissions from the PACSs, for approximately one day of noncompliance.

2. The REs determined that the Companies unnecessarily granted [REDACTED] individuals electronic access to CIP-protected information.

The violation started when the Companies granted unauthorized access and ended when the Companies revoked the unauthorized access, for approximately two months of noncompliance.

3. The REs determined that the Companies granted one individual electronic access to an [REDACTED] [REDACTED] without proper authorization.

The violation started when the Companies allowed the vendor unauthorized access to the [REDACTED] and ended the last day the vendor accessed the [REDACTED] for approximately one day of noncompliance.

4. The REs determined that the Companies improperly granted one employee electronic access to BCSs and failed to remove physical access for six individuals in accordance with their access management program.

The violation started when the Companies should have revoked the first individual's physical access and ended when the Companies revoked access for the last individual involved, for approximately nine months of noncompliance.

5. The REs determined that the Companies failed to conduct the required access verification reviews required by CIP-004-6 R4, in three instances. In the first instance, the Companies incorrectly assigned one employee to a system shared user account on an EACMS server, which affected [REDACTED] EACMS devices. In the second instance, the Companies did not identify [REDACTED] [REDACTED] as EACMSs. As a result, the Companies failed to verify: 1) access authorization records; 2) that electronic access user account groups, role categories, and specific associated privileges were correct and necessary; and 3) that designated storage for BES Cyber System Information was correct and necessary for performing work functions. In the third instance, the Companies did not identify [REDACTED] servers as EACMS. As a result, the

NERC Notice of Penalty
The Companies
January 25, 2019
Page 20

Companies failed to verify: 1) access authorization records; 2) that electronic access user account groups, role categories, and specific associated privileges were correct and necessary; and 3) that designated storage for BES Cyber System Information was correct and necessary for performing work functions.

The violation started when the Standard became mandatory and enforceable, and is currently ongoing.

The REs determined that the primary cause of the CIP-004-6 R4 violations was lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate serious and substantial risk to the reliability of the BPS.

CIP-004-6 R5

1. The REs determined that the Companies did not timely revoke eight individuals' unescorted physical access to a [REDACTED] Physical Security Perimeter (PSP) within 24 hours from termination.

The violation started when the Companies should have revoked the former contractors' physical access rights and ended when the Companies revoked the access rights, for approximately five months of noncompliance.

2. The REs determined that the Companies did not timely revoke individuals' unescorted physical access to BCSs within 24 hours of termination, in two instances. In the first instance, an employee's employment ended but the Companies did not revoke the former employee's unescorted physical access to [REDACTED] PSPs for approximately two days. In the second instance, the Companies did not revoke a former employee's unescorted physical access to [REDACTED] PSPs for approximately 20 days.

The violation started when the Companies should have revoked the former employee's unescorted physical access rights, in the first instance, and ended when the Companies revoked the access rights for the employee, in the second instance, for approximately six months of noncompliance.

3. The REs determined that the Companies did not timely revoke electronic access of an individual who no longer needed such access.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 21

The violation started when the individual's access rights were required to be revoked and ended when the Companies revoked the employee's access rights, for approximately three weeks of noncompliance.

4. The REs determined that the Companies did not timely revoke electronic access of an individual who no longer needed such access. A manager submitted a request to remove an employee's existing electronic access permission and add different electronic access permissions because of a change in job duties. The Companies' [REDACTED] tool did not allow both provision and revocation of access on the same request.

The violation started when the Companies were required to revoke the individual's access and ended when the Companies revoked the individual's access, for approximately one day of noncompliance.

5. The REs determined that the Companies did not timely revoke seven individuals' electronic access rights following their reassignments or transfers where access was no longer needed.

The violation started when the Companies were first late in revoking electronic access rights from the secondary server and ended when the Companies removed all seven individuals' electronic access rights from the secondary server, for approximately 16 months of noncompliance.

6. The REs determined that the Companies did not timely revoke one individual's electronic access following reassignment where access was no longer needed. A manager entered access revocation information in the software system used to manage CIP access; however, the revocation of access did not occur because the owner of the CIP repository failed to perform additional steps required to complete the access revocation.

The violation started when the Companies were required to revoke the employee's electronic access to the CIP repository and ended when the Companies revoked the employee's electronic access to the repository, for approximately six months of noncompliance.

7. The REs determined the Companies failed to implement the access revocation requirements of CIP-004-6 R5, in three instances. In the first instance, the Companies did not timely revoke electronic access of individuals who no longer needed such access. In the second instance, the Companies did not identify [REDACTED] as EACMSs. In the third instance, the Companies did not identify [REDACTED] servers as EACMSs.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 22

The violation started when, in the second and third instances, the Standard became mandatory and enforceable and the Companies failed to provide the protective measures required by CIP-004-6 R4, and is currently ongoing.

The REs determined the primary cause of the CIP-004-6 R5 violations was lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-005-1 (and 3a) R1

1. The REs determined that the Companies failed to identify and protect a non-critical Cyber Asset (non-CCA) within a defined Electronic Security Perimeter (ESP).

The violation started when the Standard became mandatory and enforceable and ended when the Companies placed the [REDACTED] on the CCA list and afforded the [REDACTED] the required CIP-005-3 protective measures, for approximately 69 months of noncompliance.

2. The REs determined that the Companies failed to identify and protect a non-CCA within a defined ESP. A [REDACTED] was connected to the ESP, but was not identified and afforded the protective requirements of CIP-005-3.

The violation started when the Companies connected the [REDACTED] to the ESP and ended when the Companies disconnected the [REDACTED] from the ESP, for approximately two weeks of noncompliance.

3. The REs determined the Companies failed to identify and protect a non-CCA within a defined ESP, in two instances. In both instances, a security specialist at a [REDACTED] disconnected a network cable from the back of a CCA and plugged it into his laptop.

The violation started when the security specialist plugged the laptop into the ESP, in the first instance, and ended when the security specialist removed the laptop from the ESP, for approximately one day of noncompliance.

4. The REs determined that the Companies failed to afford the protective measures in CIP-007-3a R5.1.3. to EACM devices that were not included in the 2014 CIP-007-3 R5 account verification review.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 23

The violation started when the 2014 annual period expired and the Companies had not performed an account verification review of the EACM devices and ended when the Companies completed the EACM account verification review, for approximately seven months of noncompliance.

5. The REs determined that the Companies failed to afford the protective measures specified in CIP-005-3a R3 to one EACM Cyber Asset. One firewall, serving as an EACM CA, was not sending the security event logs to the centralized system logging and monitoring (syslog) server because a network card hardware failure occurred at the firewall, preventing the firewall from sending security event logs to the centralized server.

The violation started when electronic access monitoring and logging of the firewall ceased and ended when electronic access logging and monitoring of the firewall resumed, for approximately two months of noncompliance.

6. The REs determined that the Companies failed to afford the protective measures specified in CIP-007 R6. The Companies deployed new access control lists (ACLs) to [REDACTED] electronic access points on [REDACTED] EACM device routers. The routers were misconfigured, causing the electronic access points to block the centralized logging and monitoring server logs associated with the [REDACTED] from being sent to the security incident and event management (SIEM) device.

The violation started when electronic access logging and monitoring of the [REDACTED] ceased and ended when electronic access logging and monitoring of the [REDACTED] resumed, for approximately 24 weeks of noncompliance.

The REs determined the primary cause of the CIP-005-1 and -3a R1 violations was lack of managerial oversight. The contributing causes included deficient processes, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-005-5 R1

1. The REs determined that the Companies did not deploy deny-access-by-default rules on [REDACTED] ESP firewalls, in two instances. In both instances, the Companies failed to configure the ACLs to limit the hosts from the non-ESP networks to the CAs within the ESP.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 24

The violation started when the Standard became mandatory and enforceable and ended when the Companies reconfigured the ACLs to limit access, for approximately 20 weeks of noncompliance.

2. The REs determined that the Companies did not restrict inbound electronic access to [REDACTED] ESPs. Inbound and outbound access control permissions on [REDACTED] firewalls were configured to allow connections to “any” host. The firewall management team deleted [REDACTED] network objects created for frequently used definitions from the destination field of the Companies’ firewall policy. As a result, the software defaulted to “any” access permissions.

The violation started when the Companies deleted the network objects prompting the firewall software to default to “any” access permissions and ended when the Companies updated the firewall rules to restrict inbound access, for approximately four months of noncompliance.

3. The REs determined that the Companies did not deny inbound and outbound access for unnecessary Internet Protocol (IP) addresses associated with ESP access points. [REDACTED] retired BCA IP addresses were not removed from the associated firewall rulesets.

The violation started when the Companies retired the BCAs but did not remove the related IP addresses from the associated firewall rulesets and ended when the Companies decommissioned the [REDACTED] network environment associated with the firewalls in question, for approximately 45 weeks of noncompliance.

4. The REs determined that the Companies did not monitor for malicious communications from an ESP. The Companies’ intrusion detection system (IDS) test access points (TAPs) were not monitoring ESP inbound and outbound communications because the Companies failed to properly connect the IDS TAPs cables to the new data network [REDACTED]

The violation started when the Companies improperly connected the IDS TAPs cables to the data network [REDACTED] preventing monitoring for malicious communications and ended when the Companies properly connected the IDS TAPs cables to the new data network [REDACTED] and confirmed monitoring for malicious ESP communications was fully implemented, for approximately seven weeks of noncompliance.

The REs determined the primary cause of the CIP-005-5 R1 violations was lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined the violations posed an aggregate serious risk to the reliability of the BPS.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 25
CIP-005-3a R2

1. The REs determined that the Companies did not implement organizational processes and technical and procedural mechanisms for controlling electronic access at all electronic access points to ESPs. The Companies used overly broad ESP firewall rulesets, which permitted access across ports and services that were not required for operations or for monitoring CAs within the ESPs. Additionally, the Companies failed to implement strong technical controls to ensure the authenticity of the accessing party for [REDACTED] individuals who were granted unauthorized access to the ESPs.

The violation started the day following the previous CIP Compliance Audit and ended when the Companies reconfigured the firewall rulesets preventing unauthorized access into the ESPs, for approximately 24 weeks of noncompliance.

2. The REs determined that the Companies failed to disable one port that was not required for the operation or monitoring of CAs within the ESP. The firewall ruleset previously used to connect a printer inside the [REDACTED] ESP to a corporate print server was no longer required. The old printer was replaced with a different model. The port used for the old printer was no longer required, but the Companies failed to disable the port.

The violation started when the printer port was no longer needed and ended when the Companies disabled the unnecessary port, for approximately 15 months of noncompliance.

3. The REs determined that the Companies failed to update the CCA list for personnel with authorized cyber or unescorted physical access to their EACM servers within seven days of a change in access rights. The Companies removed [REDACTED] unique user account to [REDACTED] EACM servers, provisioned access for a user account to [REDACTED] EACM server, provisioned a shared user account on [REDACTED] EACM servers for resetting passwords and support changes, and provisioned a shared user account on [REDACTED] EACM server that provided access for [REDACTED] support administrations. However, the Companies did not update the CCA access list to reflect these changes in access rights.

The violation started the earliest date the Companies provisioned access to an account but did not update the CCA access list and ended when the Companies updated the CCA access list to include all changes of access rights, for approximately 30 months of noncompliance.

The REs determined that the primary cause of the CIP-005-3a R2 violations was a lack of managerial oversight. The contributing causes included a deficient electronic access control process, inadequate training, and lack of internal controls.

NERC Notice of Penalty

The Companies

January 25, 2019

Page 26

The REs determined that the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-005-5 R2

1. The REs determined that the Companies allowed interactive remote access to BES Cyber Systems inside the Companies' ESP without first going through an Intermediate System, in two instances. In the first instance, the Companies permitted interactive remote access between [REDACTED] and the [REDACTED] without first going through an Intermediate System. In the second instance, the Companies discovered [REDACTED] that the Companies did not identify as Intermediate Systems in its initial identification assessment when transitioning to CIP version 5.

The violation started when the Standard became mandatory and enforceable and is currently ongoing.

2. The REs determined that the Companies configured firewall rulesets to allow external interactive remote access to [REDACTED] at [REDACTED] without first going through an Intermediate System.

The violation started when the Standard became mandatory and enforceable and is currently ongoing.

3. The REs determined that the Companies allowed interactive remote access to BCSs inside the Companies' ESPs without first going through an Intermediate System. The Companies configured firewall rulesets to allow [REDACTED] interactive remote access to BCSs inside the [REDACTED] ESPs without first going through an Intermediate System.

The violation started when the standard became mandatory and enforceable, and ended when the Companies changed the firewall rulesets to preclude the [REDACTED] from directly accessing BCSs inside the ESPs, for approximately nine months of noncompliance.

4. The REs determined that the Companies allowed interactive remote access to BCSs inside the Companies' ESP without first going through an Intermediate System, utilizing encryption, and requiring multi-factor authentication.

The violation started when the Standard became mandatory and enforceable and is currently ongoing.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 27

5. The REs determined that the Companies' personnel used [REDACTED] to initiate interactive remote access to [REDACTED] inside the ESPs at a [REDACTED] and [REDACTED] without first going through an Intermediate System. The Companies incorrectly configured the firewalls to grant access to a wide range of ports, include the port range used for interactive remote access.

The violation started when the Standard became mandatory and enforceable, and ended when the Companies disabled the port range firewall rule that was used for interactive remote access.

The REs determined that the primary cause of the CIP-005-5 R2 violations was a lack of managerial oversight. The contributing causes included a deficient interactive remote access management process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate serious and substantial risk to the reliability of the BPS.

CIP-006-3c R1

1. The REs determined the Companies failed to maintain a completely enclosed six-wall PSP border after the completion of a facility upgrade. A construction contractor left vents unsecured on the PSP border.

The violation started when the Companies' contractor completed the work without securing the vent openings and ended when the Companies secured the vent openings, for approximately two weeks of noncompliance.

2. The REs determined that the Companies failed to properly provision physical access authorization requests in accordance with CIP-004-3 R4.1, in four instances. In the first instance, an access services employee properly approved and granted the employee's access to the [REDACTED] PSP; however, the employee mistakenly approved and granted access to a [REDACTED] PSP instead of the non-PSP server room. In the second instance, the access service team improperly granted a contractor access to the [REDACTED] PSP. In the third instance, an access services employee erroneously approved and granted the requested access prior to the approval of the employee's manager. In the fourth instance, even though the Companies' staff manually rejected an employee access request to add access permissions, the system approved the employee for access and authorized the badge for access to the NERC CIP-identified PSP.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 28

The violation started when, in the first instance, the Companies granted the employee unauthorized access rights to the PSP and ended when, in the fourth instance, the Companies' manager approved the access request, for approximately six months of noncompliance.

3. The REs determined that the Companies failed to document all the required information in their logbooks for visitors who accessed the Companies' PSPs as required by R1.6.1. Specifically, there were over [REDACTED] instances involving all of the Companies' PSPs with at least one missing log entry, including the escort name, escort badge number, and visitor PSP entry and exit times. Additionally, there were eight occasions where the Companies failed to continuously escort visitors within multiple PSPs as required by R1.6.2.

The violation started the earliest date the Companies failed to complete the logbook entries and is currently ongoing.

4. The REs determined the Companies did not continuously escort one visitor while inside a PSP. The Companies' employee allowed a security guard, who did not have authorized unescorted access, to be inside the PSP without a continuous escort and inappropriately designated the security guard as the escort for a contractor.

The violation started when the employee left the security guard in the PSP unescorted and ended when the security guard exited the PSP, for approximately one day of noncompliance.

The REs determined the primary cause of the CIP-006-3c R1 violations was lack of managerial oversight. The contributing causes included a deficient electronic access control process, inadequate training, and lack of internal controls.

The REs determined the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-006-6 R1

1. The REs determined that the Companies failed to implement physical access controls to allow only those personnel with authorized unescorted access to access one PSP. The Companies' employee exited a PSP; however, before the PSP door fully closed, a package delivery person without authorized PSP access swung the door open and entered the PSP.

The violation started when the unauthorized individual entered the PSP and ended when the Companies' security guard escorted the unauthorized individual outside the PSP, for approximately one day of noncompliance.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 29

2. The REs determined that the Companies failed to implement physical access controls to allow only those personnel with authorized unescorted access to access [REDACTED] substation PSPs.

The violation started when the Companies granted all of the employees unauthorized physical access to the newly commissioned PSPs and ended when the Companies revoked the unauthorized access, for approximately six weeks of noncompliance.

3. The REs determined that the Companies failed to monitor for unauthorized access through a physical access point into a PSP.

The violation started when the Companies disabled alarming and monitoring at the access point and ended when the Companies re-enabled alarming and monitoring at the access point, for approximately five days of noncompliance.

4. The REs determined that the Companies failed to prevent an employee from entering a PSP. The employee did not have their employee badge, and did not manually complete the PSP visitor access log when entering the PSP.

The violation started when the employee entered the PSP without logging their access and ended when the employee exited the PSP, for approximately one day of noncompliance.

The REs determined the primary cause of the CIP-006-3c R1 violations was lack of managerial oversight.

The REs determined the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-006-3c R2

1. The REs determined that the Companies failed to review [REDACTED] individual PACS user accounts to verify that the access permissions were consistent with what the employees needed to access to perform their respective functions. The violation affected [REDACTED] PACS servers, [REDACTED] of which were deployed in the [REDACTED] while the remaining [REDACTED] were in the [REDACTED]

The violation started when the Companies were required to conduct an annual review of PACS user accounts and ended when the Companies conducted the annual review of PACS user accounts, for approximately nine months of noncompliance.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 30

2. The REs determined that the Companies did not update their CCA access list within seven calendar days of a change in access rights of personnel.

The violation started seven days after the Companies made changes to the access rights of personnel without updating their CCA access list and ended when the Companies updated the CCA access list to reflect the personnel changes, for approximately 19 months of noncompliance.

The REs determined the primary cause was a lack of managerial oversight. The contributing causes included a deficient security patch management process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate minimal risk to the reliability of the BPS.

CIP-006-6 R2

1. The REs determined that the Companies failed to continuously escort a visitor while the visitor was inside a PSP. An authorized escort was escorting a visiting contractor in the [REDACTED] [REDACTED] to perform janitorial services when they noticed a spill on the break room floor and left the PSP to get cleaning supplies. The authorized escort left the visitor unescorted inside the PSP during this time.

The violation started when the Companies' escort left the visitor unescorted and ended when the escort returned to the visitor, for approximately one day of noncompliance.

2. The REs determined that the Companies did not maintain complete access logs for [REDACTED] PSP. The Companies' employee, who had authorized access to the PSP, escorted two visitors into a [REDACTED]. The employee failed to document the visitors' entry and exit times within the PSP in the logbook.

The violation started when the employee entered the PSP with the two visitors without first documenting their entry in the logbook and ended when the employee and visitors exited the PSP, for approximately one day of noncompliance.

3. The REs determined that the Companies failed to log all required information for visitors who accessed PSPs on five different instances. In the first four instances, the Companies failed to manually log the exit times of visitors who accessed the PSPs. In the fifth instance, the Companies failed to manually log the name of the escort for a visitor who accessed a PSP.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 31

The violation started when the Companies failed to manually log the exit time of the visitor in the first instance and ended when the Companies failed to manually log the escort name in the fifth instance, for approximately two months of noncompliance.

4. The REs determined that the Companies failed to log all required information for visitors who accessed PSPs in two instances. In both instances, the Companies failed to manually log the exit time of an escorted visitor who accessed a PSP.

The violation started when the Companies failed to manually log the exit time of the visitor in the first instance and ended when the Companies failed to manually log the exit time of the visitor in the second instance, for approximately one week of noncompliance.

5. The REs determined that the Companies failed to log all required information for a visitor who accessed a PSP. The Companies failed to manually log the exit time of a visitor who accessed a [REDACTED] PSP.

The violation started and ended when the visitor exited the PSP and the Companies failed to log the exit time, for approximately one day of noncompliance.

6. The REs determined that the Companies failed to log all required information for visitors who accessed a PSP. The Companies' employee erroneously entered the visitor name for two visitors who needed access to a [REDACTED] PSP. As a result, the employee failed to log in and log out the two PSP visitors.

The violation started and ended when the employee failed to log in and log out the two PSP visitors, for approximately one day of noncompliance.

7. The REs determined that the Companies failed to log all required information for a visitor who accessed a PSP. The Companies' escort failed to properly sign out two visitors in the logging system when they left a PSP.

The violation started and ended when the escort failed to complete the log out process for the two visitors, for approximately one day of noncompliance.

8. The REs determined that the Companies failed to log all required information for a visitor who accessed a PSP. An employee failed to log an escorted visitor's exit date and time when the visitor left the PSP.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 32

The violation started and ended when the employee failed to log the exit date and time of the visitor, for approximately one day of noncompliance.

The REs determined the primary cause of the violations was a lack of managerial oversight.

The REs determined that the violations posed an aggregate moderate risk to the reliability of the BPS.

CIP-006-3c R4

The REs determined that the Companies failed to implement operational or procedural controls to manage physical access to a PSP as required by CIP-006-3c R4. The Companies' employee entered a PSP without authorized unescorted access permissions by using an emergency override key provided by the [REDACTED] operation department.

The violation began when the unauthorized technician accessed the PSP and ended when the technician exited the PSP, for approximately one day of noncompliance.

The REs determined the primary cause of the violation involved insufficient training.

The REs determined that the violation posed a moderate risk to the reliability of the BPS.

CIP-006-3c R5

1. The REs determined that the Companies failed to immediately review unauthorized physical access attempts at a PSP. An employee of the Companies made seven unauthorized physical access attempts to the PSP within one minute, despite not having authorized access. The security monitoring staff failed to contact appropriate personnel so that the unauthorized access attempts could be investigated.

The violation started when the Companies failed to immediately review the unauthorized access attempts at the PSP and ended when the Companies reviewed the unauthorized access attempts, for approximately one day of noncompliance.

2. The REs determined that the Companies failed to continuously monitor physical access at [REDACTED] access points to a PSP. [REDACTED] "exit-only" doors at one of the [REDACTED] were not sending notification to the security command center alerting when the doors were opened.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 33

The violation started when the Companies' [REDACTED] device malfunctioned and stopped sending notifications to the security command center and ended when the Companies repaired the [REDACTED] for approximately two weeks of noncompliance.

3. The REs determined that the Companies failed to immediately review unauthorized physical access attempts at a PSP. An employee of the Companies mistakenly placed the alarm for a [REDACTED] PSP badge reader into bypass mode, preventing additional alarms from being issued when an unauthorized physical access attempt occurred. Five total alarms were not issued due to this incident.

The violation started when the employee disabled the alarm and ended when the Companies review the unauthorized access attempts, for approximately five days of noncompliance.

4. The REs determined that the Companies failed to continuously monitor physical access at [REDACTED] access points to a PSP. An employee of the Companies failed to configure the PACS in alignment with the installed vendor software, preventing notifications from being sent to the security command center whenever two "exit-only" doors at the PSP was opened. As a result, the security command center was not notified whenever the doors were opened.

The violation started when the monitoring and alarming functionality for the [REDACTED] PSP doors stopped and ended when the Companies reconfigured the PACS so the monitoring and alarming functionalities for the [REDACTED] PSP doors resumed, for approximately six months of noncompliance.

5. The REs determined that the Companies failed to continuously monitor physical access to PSPs in two instances. In the first instance, there was a delay between when the PACS issued an alarm and the time the alarm appeared on the SOC monitoring consoles. In the second instance, the SOC lost power and failed over the PACS applications to a secondary site, which allowed the Companies to continue to monitor PACS alarms. However, the PACS queued the alarms and failed to forward the alarms to the SOC for acknowledgement or action.

The violation started when the Companies began deploying the new PACS and ended when the Companies commissioned a new server and implemented applicable patches, for approximately 41 weeks of noncompliance.

The primary cause of the violations was lack of managerial oversight.

The REs determined that the violation posed an aggregate serious risk to the reliability of the BPS.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 34
CIP-007-3a R1

1. The REs determined that in multiple instances the Companies failed to adhere to their cyber security testing procedures. The Companies failed to implement a cyber security testing plan in a manner that minimized adverse effects on the production system or its operation. Specifically, the Companies performed deficient testing on software upgrades for [REDACTED] CCAs in four separate instances. Additionally, the Companies failed to document the results of these deficient tests.

The violation started when the Companies first performed the deficient testing on software upgrades and ended when the Companies successfully completed their change management process for the devices involved, for approximately nine months of noncompliance.

2. The REs determined that, in five instances, the Companies failed to implement changes to existing CAs and CCAs within an ESP without testing the changes first to ensure they would not adversely affect existing cyber security controls.

In the first instance, the Companies installed software on [REDACTED] CAs, [REDACTED] of which were CCAs, without first performing the required testing to ensure the changes would not adversely affect the existing cyber security controls.

In the second instance, the Companies submitted a change management ticket to begin an operating system upgrade to an EACMS. However, the employee did not categorize the device as a NERC CIP device in the change management ticket. Therefore, the software did not initiate the testing workflow. As a result, the Companies did not complete the required cyber security controls testing before the operating system upgrade was completed.

In the third instance, the Companies replaced [REDACTED] CCAs at a [REDACTED] without conducting a cyber security control test. Additionally, the Companies failed to update the device list software or communicate the changes to the engineering department. As a result, the Companies did not update the changes in their database, which was used to track the information of the CCAs.

In the fourth instance, the Companies performed a firmware upgrade to a programmable automation controller without conducting cyber security testing on the asset prior to implementation. In addition, once the firmware upgrade was completed, the Companies did not update the device list software or communicate the changes to the engineering department.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 35

In the fifth instance, the Companies installed a new CCA for an upgrade on a [REDACTED] without conducting a cyber security control test or maintaining sufficient change management documentation.

The violation started when, in the fifth instance, the Companies installed a new device without performing a cyber security controls test and ended when the Companies completed the cyber security controls test, for approximately 16 months of noncompliance.

3. The REs determined that the Companies failed to implement their cyber security test procedures for [REDACTED] CA. The Companies deployed a port server, which allowed access to the serial port of another device over Transmission Control Protocol/Internet Protocol, inside an ESP without first testing the server to ensure it did not adversely affect existing cyber security controls.

The violation started when the Companies failed to conduct a cyber security test before deploying the port server and ended when the server was tested, for approximately 15 months of noncompliance.

The primary cause of the violations was lack of managerial oversight.

The REs determined that the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-007-6 R1

The REs determined that the Companies failed to enable only the necessary logical network accessible ports, in three instances. In the first instance, the Companies never implemented the security patch management program on [REDACTED] devices because they failed to identify them as EACMS devices. In the second instance, that the Companies enabled unnecessary logical network accessible points because they had failed to identify [REDACTED] as EACMSs. In the third instance, the Companies enabled unnecessary logical network accessible ports because they had failed to identify [REDACTED] servers as EACMSs.

The violation began when the Standard became mandatory and enforceable and is currently ongoing.

The primary cause of the violation was insufficient training.

The REs determined that the violation posed a moderate risk to the reliability of the BPS.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 36
CIP-007-6 R2

1. The REs determined that the Companies failed to monitor for vendor security patches and vulnerability notifications for an application on ██████ BCAs.

The violation began when the Standard became mandatory and enforceable and ended when the Companies began monitoring for patches for the BCAs, for approximately 18 months of noncompliance.

2. The REs determined that the Companies failed to conduct timely evaluations of ██████ security patches. In two instances, the Companies' patch vendor submitted ██████ security patches for applicability evaluations. The employee who received the notifications sent emails to the personnel responsible for conducting the evaluations, requesting that the Companies conduct the evaluations. The Companies failed to conduct the evaluations.

The violation began when the Companies were first required to conduct a patch evaluation and ended when the Companies conducted evaluations for both patches, for approximately one month of noncompliance.

3. The REs determined that the Companies failed to conduct timely patch evaluations for ██████ security patches relating to EACMSs and ██████ associated medium impact BCAs.

The violation began when the Companies were required to conduct the patch evaluations and ended when the Companies conducted the patch evaluations, for approximately seven weeks of noncompliance.

4. The REs determined that the Companies failed to conduct timely patch evaluations for ██████ security patches. The Companies were unaware of ██████ security patches that the vendor released because the vendor's website had relocated the information to a different section of its website.

The violation began when the Companies failed to conduct the patch evaluation and ended when the Companies conducted patch evaluations for all ██████ patches, for approximately 11 months of noncompliance.

5. The REs determined that the Companies failed to implement their security patch management program in four different instances. In the first instance, the Companies failed to apply ██████ applicable security patches and failed to implement compensating measures to mitigate detected vulnerabilities. In the second instance, the Companies failed to identify ██████ EACMS

NERC Notice of Penalty
The Companies
January 25, 2019
Page 37

devices, which each protected a [REDACTED] and were deployed outside the ESP. As a result, the Companies failed to implement their security patch management program on these EACMSs. In the third instance, the Companies failed to identify [REDACTED] as EACMSs, and as a result failed to implement their security patch management program on them. In the fourth instance, the Companies failed to identify [REDACTED] servers as EACMSs, and as a result failed to implement their security patch management program on them.

The violation started when the Standard became mandatory and enforceable and is currently ongoing.

The REs determined the primary cause was a lack of managerial oversight. The contributing causes included a deficient security patch management process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-007-3a R3

1. The REs determined that the Companies failed to assess [REDACTED] security patches for [REDACTED] within 30 days of their availability.

The violation started when the Companies failed to assess the first available security patch within 30 days of its release and ended when the Companies assessed all available security patches, for approximately five months of noncompliance.

2. The REs determined that the Companies failed to install a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all CAs within an ESP. The Companies transferred the responsibility of monitoring for available security patches and vulnerabilities from the [REDACTED] Team to their Telecom Team. In this transfer of responsibility, the Telecom team failed to monitor vendor security patches and vulnerability notifications. The security vulnerabilities affected [REDACTED]

The violation started when the Companies failed to assess the first available security patch within 30 days and ended when the Companies decommissioned the [REDACTED] affected [REDACTED] for approximately 28 months of noncompliance.

The REs determined the primary cause was a lack of managerial oversight. The contributing causes included a deficient security patch management process, inadequate training, and lack of internal controls.

NERC Notice of Penalty

The Companies

January 25, 2019

Page 38

The REs determined that the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-007-6 R3

The REs determined that the Companies failed to implement methods to deter, detect, or prevent malicious code, including having a process for methods that use signatures or patterns to update those signatures and patterns. The Companies tested and installed antivirus signatures for all BCAs in [REDACTED] facility, but were unable to provide evidence demonstrating that they used a process to update the signatures. The violation affected [REDACTED] medium impact BES Cyber System that consisted of [REDACTED] BCAs and [REDACTED] EACMSs.

The violation started when the Companies failed to document their testing and installing of signatures and ended when the Companies began documenting their testing and installing of signatures, for approximately 20 weeks of noncompliance.

The REs determined the primary cause was a lack of managerial oversight and inadequate internal controls. Specifically, there was no process in place for generating CIP compliance tasks, so the compliance analyst could not effectively perform evaluations and store the evidence.

The REs determined that the violation posed a moderate risk to the reliability of the BPS.

CIP-007-6 R4

1. The REs determined that the Companies failed to implement security event monitoring for multiple CAs, in four separate instances.

In the first instance, the Companies failed to implement security event logging for [REDACTED] [REDACTED] that were associated with [REDACTED]. While looking into the issue, the Companies discovered [REDACTED] additional instances of the same issue at multiple medium impact [REDACTED].

In the second instance, the Companies failed to identify [REDACTED] as EACMSs. Due to this failure, the EACMSs did not generate alerts for security events, and the Companies did not review logged events for cyber security events.

In the third instance, the Companies failed to identify [REDACTED] servers as EACMSs. Due to this failure, the EACMSs did not generate alerts for security events, and the Companies did not review logged events for cyber security events.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 39

In the fourth instance, the Companies failed to identify [REDACTED] device as a Protected Cyber Asset (PCA). Due to this failure, the Companies did not implement security event logging for the PCA.

The violation started when the Standard became mandatory and enforceable and is currently ongoing.

2. The REs determined that the Companies failed to review a summarization of logged events at least every 15 calendar days to identify undetected Cyber Security Incidents.

The violation started when the Companies were required to conduct a review of logged events and ended when the Companies conducted a review of the logged events, for approximately two weeks of noncompliance.

The REs determined the primary cause of the violations was lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the CIP-007-6 R4 violations posed an aggregate serious risk to the reliability of the BPS.

CIP-007-3a R5

1. The REs determined that a service technician at the Companies was sharing his username and password to access devices inside the [REDACTED] with two team-member service technicians who did not have authorized electronic access to the devices.

The violation started when the two service technicians gained unauthorized access to CAs inside the [REDACTED] by utilizing the authorized technician's individual user account credentials and ended when the authorized employee changed his individual user account password, for approximately 33 months of noncompliance.

2. The REs determined that the Companies failed to document an application account deployed on [REDACTED] EACMSs in [REDACTED] that housed high impact BES Cyber Systems.

The violation started when the Companies created the system shared account and ended when the Companies identified and began managing the scope and acceptable use of the system shared user account, for approximately two years of noncompliance.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 40

3. The REs determined that the Companies' "read-only" passwords on a single [REDACTED] within one of the [REDACTED] remained unchanged after the expiration of the mandatory annual password changed deadline.

The violation started when the Companies were required to have changed the [REDACTED] passwords and ended when the Companies changed the passwords, for approximately six months of noncompliance.

4. The REs determined that the Companies did not change factory default passwords for remotely accessible BCAs in [REDACTED] instances.

The violation started when the Standard became mandatory and enforceable and ended when the Companies changed the last of the factory default passwords, for approximately 74 months of noncompliance.

The REs determined the primary cause of the violations was lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-007-6 R5

1. The REs determined that the Companies failed to implement system access controls to CAs within ESPs in accordance with CIP-007-6 R5, in four instances. In the first instance, the Companies did not request a Technical Feasibility Exception (TFE) for [REDACTED] of [REDACTED] CAs associated with [REDACTED] high impact BCSs. In the second instance, the Companies did not identify [REDACTED] as EACMSs. This instance affected [REDACTED] high impact BCSs, which consisted of [REDACTED] EACMSs. In the third instance, the Companies did not identify [REDACTED] servers as EACMSs. This instance affected [REDACTED] EACMSs and [REDACTED] PACs, all associated with high impact BCSs. In the fourth instance, the Companies did not identify [REDACTED] device as a PCA. This instance affected a high [REDACTED], which contained [REDACTED] BCAs, [REDACTED] EACMSs, and [REDACTED] PCAs.

The violation started when the Standard became mandatory and enforceable and is currently ongoing.

2. The REs determined that the Companies did not identify and inventory enabled default accounts associated with [REDACTED] communications processors at [REDACTED]

NERC Notice of Penalty
The Companies
January 25, 2019
Page 41

The violation started when the Standard became mandatory and enforceable and is currently ongoing.

3. The REs determined that the Companies' password management tool (PMT) was not correctly managing [REDACTED] BCAs. The PMT lost communications with these [REDACTED] BCAs, which went unnoticed because it did not affect the functionality of the BCAs.

The violation started when the Companies were required to change the passwords to the [REDACTED] BCAs and ended when the Companies changed the password on the last BCA, for approximately six months of noncompliance.

The REs determined the primary cause of the CIP-007-6 R5 violations was lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined the CIP-007-6 R5 violations posed an aggregate serious risk to the reliability of the BPS.

CIP-007-3a R6

The REs determined that the Companies failed to ensure that security monitoring controls issued automated or manual alerts for detected Cyber Security Incidents. When the Companies implemented a new [REDACTED] tool, they made a configuration error that prevented email alerts from being sent to response personnel for detected Cyber Security Incidents.

The violation started when the Companies misconfigured the [REDACTED] tool and ended when the Companies reconfigured the [REDACTED] tool and alerting for unsuccessful login attempts resumed, for approximately 28 weeks of noncompliance.

The REs determined the primary cause of the violation was lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and a lack of internal controls.

The REs determined that the violation posed a moderate risk to the reliability of the BPS.

CIP-007-3a R7

The REs determined that the Companies failed to implement their internal disposal and redeployment program, which requires the device to remain within the designated PSP until a proper chain of custody process is followed to transport the device in a secured container to the appropriate sanitizing facility, in two instances.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 42

The violation started when, in the first instance, the Companies' employee transported the device without properly securing it and ended when, in the second instance, the Companies received the device at the sanitizing location and sanitized it, for approximately one week of noncompliance.

The REs determined that the primary cause of the violation was an inadequate process.

The REs determined that the violation posed a minimal risk to the reliability of the BPS.

CIP-007-3a R8

The REs determined that the Companies failed to document a Cyber Vulnerability Assessment (CVA) action plan to remediate or mitigate vulnerabilities. After the Companies completed their annual CVA on CAs associated with a [REDACTED] and [REDACTED] the Companies' IT support team identified vulnerabilities but did not create a formal mitigation action plan to remediate or mitigate identified vulnerabilities.

The violation started when the Companies failed to document the CVA vulnerability action plan and ended when the Companies documented the vulnerability action plan, for approximately four months of noncompliance.

The REs determined that the primary cause of the violation was ineffective training.

The REs determined that the violation posed a moderate risk to the reliability of the BPS.

CIP-007-3a R9

The REs determined that the Companies failed to document modifications to systems and controls of a CA within an ESP within 30 calendar days. The Companies failed to report within 30 calendar days when they replaced a communications processor connected to a modem with a working phone line, leaving the modem in place and attaching it to a different CCA.

The violation started 30 days after the Companies made modifications to systems and controls and did not document the modifications and ended when the Companies removed the modem from service, for approximately 13 months of noncompliance.

The REs determined that the primary cause of the violation was a lack of training.

The REs determined that the violation posed a minimal risk to the reliability of the BPS.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 43
CIP-009-6 R1

The REs determined that the Companies failed to include EACMSs in their documented Recovery Plan in two separate instances. In the first instance, the Companies did not identify [REDACTED] as EACMSs, therefore failing to include them in their documented Recovery Plan. In the second instance, the Companies did not identify [REDACTED] servers as EACMSs, therefore failing to include them in their documented Recovery Plan.

The violation started when the Standard became mandatory and enforceable and ended when the Companies included the EACMSs in their Recovery Plan, for approximately 21 months of noncompliance.

The REs determined that the primary cause of the violation was a lack of managerial oversight. The contributing cause was inadequate training.

The REs determined that the violation posed a moderate risk to the BPS.

CIP-009-6 R2

The REs determined that the Companies failed to include EACMSs in the implementation and subsequent testing of the documented Recovery Plan in two separate instances. In the first instance, the Companies did not identify [REDACTED] servers as EACMSs. In the second instance, the Companies did not identify [REDACTED] as EACMSs.

The violation started when the standard became mandatory and enforceable and ended when the Companies included the EACMSs in the implementation and testing of their Recovery Plan, for approximately 21 months of noncompliance.

The REs determined that the primary cause of the violation was a lack of managerial oversight. The contributing cause was inadequate training.

The REs determined that the violation posed a moderate risk to the BPS.

CIP-009-6 R3

The REs determined that the Companies failed to include EACMSs in the reviews and updates of their Recovery Plan, in three separate instances. In the first instance, the Companies failed to include PCAs in the documented Recovery Plan. In the second instance, the Companies failed to identify [REDACTED]

NERC Notice of Penalty

The Companies

January 25, 2019

Page 44

[REDACTED] as EACMSs. In the third instance, the Companies failed to identify [REDACTED] servers as EACMSs.

The violation started when the Standard became mandatory and enforceable and ended when the Companies included these EAMSs in the review and update of the Recovery Plan, for approximately 21 months of noncompliance.

The REs determined that the primary cause of the violation was a lack of managerial oversight. The contributing cause was inadequate training.

The REs determined that the violation posed a moderate risk to the reliability of the BPS.

CIP-010-2 R1

1. The REs determined that the Companies failed to maintain an accurate baseline configuration because they included devices in their baseline that were no longer a part of their BES Cyber System. [REDACTED] BCAs on the Companies' inventory list were decommissioned, but the Companies failed to update the BCA inventory list.

The violation started when the Standard became mandatory and enforceable and is currently ongoing.

2. The REs determined that the Companies failed to develop accurate baseline configurations. The Companies installed a different firmware version on [REDACTED] associated with PACSs than was documented in the existing baseline configurations.

The violation started when the Standard became mandatory and enforceable and ended when the Companies update their baseline configurations to reflect the firmware version installed on the [REDACTED] for approximately one year of noncompliance.

3. The REs determined that the Companies failed to develop accurate baseline configurations. The Companies failed to include [REDACTED] BCAs in their baseline configurations. Additionally, the Companies failed to include [REDACTED] BCAs and [REDACTED] PCAs in the correct baseline configurations. Moreover, the Companies incorrectly documented in their baseline configurations one port associated with [REDACTED] BCAs used by administrators as a backup to analyze events.

The violation started when the Standard became mandatory and enforceable and is currently ongoing.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 45

4. The REs determined that the Companies failed to include enabled logical network ports in their baseline configuration for [REDACTED] CA devices located at [REDACTED] different facilities.

The violation started when the Standard became mandatory and enforceable and ended when the Companies updated their baselines, for approximately two months of noncompliance.

5. The REs determined that the Companies failed to include enabled logical network accessible ports in their baseline configuration for [REDACTED] EACMS.

The violation started when the Standard became enforceable and ended when the Companies updated their baseline configuration to reflect the enabled logical network accessible ports, for approximately four months of noncompliance.

6. The REs determined that the Companies failed to include enabled logical network accessible ports in their baseline configuration. The Companies failed to include the enabled logical network accessible ports associated with a server used to run [REDACTED] software.

The violation started when the Standard became mandatory and enforceable and ended when the Companies updated their baseline to include the missing ports, for approximately 14 months of noncompliance.

7. The REs determined that the Companies failed to include two security patches in their baseline configuration. The Companies applied two patches as an upgrade to an appliance associated with [REDACTED] BCAs but failed to update the baseline configuration to reflect the changes prior to the effective date of CIP-010-2 R1; P1.1.5.

The violation started when the Standard became mandatory and enforceable and ended when the Companies updated the baseline configuration, for approximately one month of noncompliance.

8. The REs determined that the Companies failed to authorize and document changes that deviated from the existing baseline configuration. The Companies installed configuration management software on [REDACTED] BCAs at a [REDACTED] without prior authorization and documenting the changes to the existing baseline configuration.

The violation started when the Companies implemented unapproved changes to the existing baseline configuration and ended when the Companies completed the security controls testing, for approximately three weeks of noncompliance.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 46

9. The REs determined that the Companies failed to authorize and document changes that deviated from the existing baseline configuration. The Companies implemented two patches to [REDACTED] EACMSs without prior authorization and documenting the changes to the existing baseline configuration.

The violation started when the Companies implemented the unapproved changes and ended when the Companies completed the security controls testing, for approximately three weeks of noncompliance.

10. The REs determined that the Companies failed to authorize and document changes that deviated from the existing baseline configuration. The Companies' engineer installed software on [REDACTED] workstations located at a [REDACTED] without prior authorization.

The violation started when the Companies implemented the changes that deviated from the existing baseline without prior authorization and ended when the Companies authorized the request to make changes, for approximately five days of noncompliance.

11. The REs determined that the Companies failed to document cyber security controls impacted by a system upgrade, verify that the cyber security controls were not impacted, or document the results of the verification. The Companies implemented changes to a PCA that deviated from the existing baseline configuration without first determining the security controls in CIP-005 and CIP-007 that could be impacted by the changes. Following the changes to the PCA, the Companies did not verify that such cyber security controls were not adversely affected by the changes.

The violation started when the Companies failed to identify cyber security controls that could be impacted before implementing changes to existing baseline configurations and is currently ongoing.

12. The REs determined that the Companies failed to fully implement their configuration change management program, in five instances. In the first instance, the Companies did not identify cyber security controls that could be impacted before implementing changes to existing baseline configurations or verify that such controls were not adversely affected after implementing the changes. In the second instance, the Companies did not document [REDACTED] EACM devices, each of which protected a [REDACTED]. In the third instance, the Companies did not identify [REDACTED] operating as EACMSs. In the fourth instance, the Companies did not identify [REDACTED] servers as EACMSs. In the fifth instance, the Companies did not identify [REDACTED] device as a PCA.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 47

The violation started when the Standard became mandatory and enforceable and is currently ongoing.

The REs determined that the primary cause of the CIP-010-2 R1 violations was a lack of managerial oversight. The Contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-010-2 R2

1. The REs determined that the Companies failed to monitor changes to the baseline configurations at least once every 35 calendar days in two separate instances. In the first instance, the Companies failed to monitor changes to the baseline configurations for [REDACTED] EACMSs at least once every 35 calendar days. In the second instance, the REs discovered that the Companies failed to monitor for changes to baseline configurations for [REDACTED] EACMSs firewall at least once every 35 calendar days.

The violation started when the Companies were required to monitor changes to the baseline configurations and ended when the Companies monitored for changes to the baseline configurations, for approximately one month of noncompliance.

2. The REs determined that the Companies not monitor for changes to the baseline configurations for one firewall at least once every 35 calendar days. This violation affected [REDACTED] high impact facility with [REDACTED] BCAs, [REDACTED] EACMSs, and [REDACTED] PACSs.

The violation started when the Companies were required to monitor for changes and ended when the Companies monitored for changes to the baseline configuration for the firewall, for approximately six months of noncompliance.

3. The REs determined that the Companies' monitoring for changes to the baseline configurations for [REDACTED] EACMSs exceeded 35 calendar days. The violation affected [REDACTED] with [REDACTED] EACMSs and [REDACTED] associated high impact BCAs and [REDACTED] high impact PCAs.

The violation started when the Companies were required to monitor for changes to the baseline configurations for the EACMSs and ended when the Companies monitored for changes to baseline configurations, for approximately one month of noncompliance.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 48

4. The REs determined that the Companies failed to monitor baseline configurations in three instances. In the first instance, the Companies had two Intrusion Detection/Prevention System (IDS/IPS) devices that were not monitored for changes to the baseline configurations for over 35 calendar days. In the second instance, the Companies had not identified [REDACTED] as EACMSs. As a result, the Companies failed to monitor those controllers at least once every 35 calendar days for changes to the EACMSs baseline configurations and document and investigate detected unauthorized changes. In the third instance, the Companies had not identified [REDACTED] servers as EACMSs. As a result, the Companies failed to monitor at least once every 35 calendar days for changes to the EACMSs baseline configurations and document and investigate detected unauthorized changes.

The violations started when the Companies should have monitored for changes to their baseline configurations and documented and detected unauthorized changes and is currently ongoing.

The REs determined that the primary cause of the CIP-010-2 R2 violations was a lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate moderate risk to the reliability of the BPS.

CIP-010-2 R3

1. The REs determined that the Companies failed to perform an active vulnerability assessment of a PCA prior to deploying it into the production environment. The Companies' subject matter expert (SME) did not complete an active vulnerability assessment as a part of change management prior to commissioning the single PCA into an ESP, which contained [REDACTED] CAs.

The violation started when the SME commissioned a PCA to the production ESP without first completing an active vulnerability assessment and ended when the Companies removed the device from the ESP, for approximately one week of noncompliance.

2. The REs determined that the Companies failed to perform an active vulnerability assessment of [REDACTED] CAs prior to deploying them into the production environment. The Companies placed [REDACTED] EACMSs firewall appliances into the production environment without performing an active vulnerability assessment.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 49

The violation started when the Standard became mandatory and enforceable and ended when the Companies completed the vulnerability assessment on the CAs, for approximately two weeks of noncompliance.

3. The REs determined that the Companies failed to perform active vulnerability assessments before deploying a BCS and multiple BCAs into the production environment in four instances. In the first instance, a Companies' [REDACTED] SME reviewed a network anomaly report and discovered that a BCA did not have malicious software prevention tools installed when it was deployed into the production environment. In the second instance, the Companies had not documented [REDACTED] EACMSs, each protecting a [REDACTED]. In the third instance, the Companies had not identified [REDACTED] operating as EACMSs. In the fourth instance, the Companies had not identified [REDACTED] servers as EACMSs.

The violations started when the Standard became mandatory and enforceable and is currently ongoing.

The REs determined that the primary cause of the CIP-010-2 R3 violations was a lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate moderate risk to the reliability of the BPS.

CIP-010-2 R4

1. The REs determined that the Companies failed to implement one or more documented plans for Transient Cyber Assets (TCAs) in multiple instances. In the first instances, two IT support personnel were granted unauthorized access to two TCAs. In the second instance, the Companies installed and uninstalled application software to [REDACTED] TCAs without prior authorization. In the third instance, [REDACTED] TCA had at least one missing patch in violation. In the fourth instance, patch tracking documentation was unavailable for [REDACTED] TCAs. The Companies conducted an extent of condition review and discovered additional instances of unauthorized software residing on TCAs and additional instances of missing patches where the Companies failed to install certain anti-virus components on TCAs, which precluded logging [REDACTED] [REDACTED], a function often used to connect a TCA to a BCA.

The violation started when in the first and fourth instances, the Standard became mandatory and enforceable and is currently ongoing.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 50

2. The REs determined that the Companies failed to use an approved TCA when connecting to a BCA to change passwords. Two of the Companies' personnel were at a BES facility when one employee connected one of the Companies' laptops, which was not an approved TCA, to a BCA at the facility and began the process of changing [REDACTED] passwords.

The violation started when the Companies connected an unapproved laptop to a BCA and when the Companies disconnected the unapproved laptop from the BCA, for approximately one day of noncompliance.

The REs determined that the primary cause of the CIP-010-2 R4 violations was a lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate serious risk to the reliability of the BPS.

CIP-011-2 R1

1. The REs determined that the Companies failed to protect and securely handle BES Cyber System Information (BCSI) in accordance with their information protection program. A Companies' employee transferred BCSI to a vendor using [REDACTED] which is not an accepted protocol in the Companies' information protection program for transmitting BCSI.

The violation started on when the employee sent the BCSI to the vendor and ended when the vendor deleted the information, for approximately one day of noncompliance.

2. The REs determined that the Companies failed to protect and securely handle BCSI in accordance with their information protection program. The Companies' project manager emailed BCSI without labeling the information as BCSI and without using a secure method of transmittal, as prescribed in the Companies' information protection program.

The violation started and ended, on the same day, when the project manager employee sent unsecured BCSI via email, for approximately one day of noncompliance.

3. The REs determined that the Companies failed to protect and securely handle BCSI in accordance with their information protection program. The Companies' system administrator's access to [REDACTED] of their [REDACTED] total repositories had not been logged. As a result, logs were unavailable for management to review and verify for accuracy and that individuals had a business need to access BCSI repositories, as prescribed by the Companies' information protection program.

NERC Notice of Penalty
The Companies
January 25, 2019
Page 51

The violation started when the Standard became mandatory and enforceable and ended when logs became available and the Companies began reviewing and verifying the logs, for approximately 17 months of noncompliance.

4. The REs determined that the Companies failed to identify and securely handle BCSI in accordance with their information protection program in three instances. In the first instance, the Companies did not identify a software program that managed protection system testing as a BCS information repository. In the second instance, the Companies did not identify as EACMSs, thereby failing to implement identification and protection requirements on the EACMSs. In the third instance, the Companies had not identified servers as Intermediate Systems or EACMSs, thereby failing to implement the BCSI identification and protection requirements on the EACMS servers.

The violation started when the Standard became mandatory and enforceable and is currently ongoing.

The REs determined that the primary cause of the CIP-011-2 R1 violations was a lack of managerial oversight. The contributing causes included a deficient process, inadequate training, and lack of internal controls.

The REs determined that the violations posed an aggregate serious and substantial risk to the reliability of the BPS.

CIP-011-2 R2

The REs determined that the Companies failed to protect BCSI in accordance with their information protection program in three separate instances. In the first instance, the Companies had not identified EACMSs. In the second instance, the Companies did not identify as EACMSs. In the third instance, the Companies did not identify servers as EACMSs. As a result of each instance, the Companies failed to take action to prevent the unauthorized retrieval of BCSI from the CA data storage media.

The violation started on when the Standard became mandatory and enforceable and the Companies failed to provide the protections required by CIP-011-2 R2, and is currently ongoing.

The REs determined that the primary cause of the violation was insufficient training on identifying in-scope cyber assets.

NERC Notice of Penalty

The Companies

January 25, 2019

Page 52

The REs determined that the violations posed a moderate risk to the reliability of the BPS.

CIP-014-2 R1

The REs determined that the Companies failed to include all applicable [REDACTED] in their CIP-014-2 R1 risk assessment. The Companies removed a [REDACTED] from the substation list because it mistakenly determined that it was not subject to Applicability Section 4.1.1.1 of the standard. As a result, the [REDACTED] was not included in the Companies' CIP-014-2 R1 risk assessment.

The violation started when the Companies failed to include the [REDACTED] in their CIP-014-2 R1 risk assessment, and ended when the Companies completed the risk assessment reflecting the missing substation, for approximately 10 months of noncompliance.

The REs determined that the primary cause of the violation was a misapplication of the criteria in the Applicability Section of the standard when reviewing the [REDACTED] list by not applying all criteria.

The REs determined that the violation posed a moderate risk to the reliability of the BPS.

To mitigate this violation, the Companies:

1. Ran a special assessment on the substation in question and shared results with their unaffiliated third-party vendor;
2. Revisited CIP-014 best practices with other of the Companies' Transmission planning corporate affiliates; and
3. Modified and republished their CIP-014-2 methodology so that in future assessments, the Companies will include all transmission station and substations to be shared with the unaffiliated third-party verifier, making no exclusions for Applicability Section 4.1.1.

On August 25, 2017, the Companies certified that they completed the Mitigation Plan.

Regional Entities' Basis for Penalty

According to the Settlement Agreement, the REs assessed a penalty of ten million dollars (\$10,000,000) for the referenced violations. In reaching this determination, the REs considered the following factors:

NERC Notice of Penalty
The Companies
January 25, 2019
Page 53

1. The REs considered the instant violations as repeat noncompliance with the subject NERC Reliability Standards. The REs considered the Companies' compliance history with CIP-002-1 R1, R2, and R3; CIP-002-3 R3; CIP-003-1 R4, R5, and R6; CIP-003-3 R1, R4, R5, and R6; CIP-004-1 R2, R3, and R4; CIP-004-3 R2 and R4; CIP-004-3a R2 and R4; CIP-005-1 R1, R2, R3, R4, and R5; CIP-005-3 R4; CIP-005-3a R1, R2, R3, R4, and R5; CIP-006-1 R1, R2, R3, and R4; CIP-006-2 R5; CIP-006-3a R1; CIP-006-3c R1, R2, R4, R5, R6, and R8; CIP-007-1 R1, R2, R3, R4, R5, R6, and R8; CIP-007-2a R5 and R6; CIP-007-3a R1, R3, R4, R5, R6, R7, and R8; CIP-008-1 R1; CIP-009-1 R5; and CIP-009-3 R5 as an aggravating factor in the penalty determination.
2. The Companies had an internal compliance program at the time of the violations, but the REs determined that, given the difficulties described above, the quality of the Companies' compliance program was deficient in facilitating the Companies' compliance with the CIP Standards and Requirements;
3. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
4. Although the risk posed to the BPS by the individual violations ranged from minimal to serious (52 minimal, 62 moderate, and 13 serious), the collective risk of the 127 violations posed a serious risk to the reliability of the BPS, as discussed in Attachment A;
5. The REs considered the Companies' lack of management involvement as an aggravating factor for penalty purposes. The Companies' management passively accepted the Companies' prior violations by creating and allowing a culture to exist that permitted these systemic problems to continue for over five years; and
6. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, the REs determined that, in this instance, the penalty amount of ten million dollars (\$10,000,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Additional Terms and Conditions

The Settlement Agreement includes the following additional conditions:

1. The Companies' Chief Executive Officer must sign the Settlement Agreement;

NERC Notice of Penalty
The Companies
January 25, 2019
Page 54

2. The Companies must provide quarterly reports to their Board of Directors, the Chief Executive Officer, and the REs until the REs determine that said reporting is no longer necessary; and
3. The REs will perform increased compliance monitoring to monitor higher-risk areas across the Companies' program and verify the accuracy of the content within the Companies' reporting dashboard. This will include at least annual monitoring, including targeted CIP audits, spot checks, and/or self-certifications.

Statement Describing the Assessed Penalty, Sanction, or Enforcement Action Imposed⁴

Basis for Determination

The NERC BOTCC reviewed the Settlement Agreement and supporting documentation on November 6, 2018 and approved the resolution between the REs and the Companies. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

The NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of ten million dollars (\$10,000,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS. The penalty for this case will be allocated by a net energy for load (NEL) calculation based on NERC's 2017 budget. For the purposes of penalty calculation in this Agreement, the NEL values correspond to weighted penalties of [REDACTED]

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.

Nonpublic Treatment

As noted above, 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 an 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

⁴ See 18 C.F.R. § 39.7(d)(4).

NERC Notice of Penalty

The Companies

January 25, 2019

Page 55

attack on Critical Electric Infrastructure. NERC requests that the redacted portions of this filing be designated as nonpublic under Section 39.7(b)(4) and as CEII under Section 388.113.⁵

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 the public version of this Notice of Penalty according to Section 39.7(b)(4) because the disposition of these violations contains information that would jeopardize the security of the BPS if publicly disclosed.⁶ The redacted information includes the identity of the Companies and details that could lead to the identity of the Companies, and information about the security of the Companies' systems and operations, such as specific configurations or tools the Companies use 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 registered 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."⁷

Consistent with the Commission's statement, NERC is treating as nonpublic the identity of the Companies and any information that could lead to the identification of the Companies.⁸ Entities

⁵ 18 C.F.R. § 388.113(e)(1).

⁶ NERC has previously filed dispositions of CIP violations on a nonpublic basis because of this regulation. To date, the Commission has directed public disclosure regarding the disposition of CIP violations in only a small number of cases. See Freedom of Information Act Appeal, FOIA No. FY18-75 (August 2, 2018); *Southwest Power Pool, Inc.*, "Order Denying Waiver Request and Dismissing Filing," 165 FERC ¶ 61,220 (2018)(SPP Order). Based on the facts specific to 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.

⁷ *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).

⁸ See the next section for a list of this information.

NERC Notice of Penalty

The Companies

January 25, 2019

Page 56

providing electricity to the people of the United States are subject to constant attacks by malicious parties, including some supported by foreign governments.⁹ Identifying the Companies in this case would highlight entities whose implementation of the CIP standards was inadequate and may be more vulnerable to cyber attacks. Nonpublic treatment of this filing is especially appropriate because of the Companies' ongoing mitigation to remediate the large number of violations. Consistent with the purpose of Section 39.7(b)(4), NERC's Notices of Penalty should not be mechanisms for adversaries to identify more desirable targets and jeopardize the security of the BPS.¹⁰

NERC is also treating as nonpublic any information about the security of the Companies' systems and operations.¹¹ Details about an 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.¹² The Companies' operations and facilities are vitally important to the customers and geographic areas they serve. The scale and scope of the Companies' violations are also significant, creating potential vulnerabilities.

Malicious individuals already target the Companies' operational personnel, seeking bits and pieces of data to map the Companies' systems and identify possible attack vectors. The public disclosure of a single piece of redacted information may not, on its own, provide everything needed to exploit an entity and attack the electric grid. But, successive public disclosures of additional pieces of redacted information will increase the likelihood of a cyber-intrusion with a corresponding adverse effect on energy infrastructure. Each successive disclosure could fill in some knowledge gaps of those planning to do harm, helping to complete the maps of entity systems. Therefore, it is important to examine and evaluate the redacted information in the aggregate.

As noted above, NERC's Notices of Penalty should not become mechanisms for adversaries to obtain information about an entity's systems or security configurations and tools to aid in perpetrating a cyber attack. As the Commission has stated, "[g]uarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure."¹³

⁹ Rebecca Smith and Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It," *Wall Street Journal* (January 11, 2019)(<https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-door-and-russia-walked-through-it-11547137112>).

¹⁰ See *Order No. 672* at P 538.

¹¹ See the next section for a list of this information.

¹² See "America's Electric Grid Has a Vulnerable Back Door" (detailing phishing and other hacking schemes aimed at utility contractors in order to penetrate utility networks).

¹³ *Reliability Standards for Physical Security Measures*, "Order Directing Filing of Standards," 146 FERC ¶ 61,166 at P 10 (2014).

NERC Notice of Penalty
The Companies
January 25, 2019
Page 57

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

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 Companies' critical infrastructure. The incapacity or destruction of the Companies' systems and assets would negatively affect national security, economic security, and public health and safety. For example, the information includes the identification of specific cyber security issues and vulnerabilities, as well as details concerning the types and configurations of the entities' systems and assets. The information also describes strategies, techniques, and solutions used to resolve specific cyber security issues.

In addition to the names of the Companies, the following information has been redacted from this Notice of Penalty as CEII as the information, when viewed collectively, could be useful to a person planning an attack:

1. BES Cyber System Information, including security procedures and information related to BES Cyber Assets.
2. The names of the Companies' vendors and contractors.
3. The NERC Compliance Registry numbers of the registered entities.
4. The registered functions and registration dates of the registered entities.
5. The names of registered entity facilities.
6. The names of registered entity assets.
7. The names of registered entity employees.
8. The names of departments that are unique to the registered entity.
9. The sizes and scopes of the registered entities' operations.
10. The dates of Compliance Audits of the registered entities, as those dates are included in schedules published by the Regional Entities.
11. The dates of Self-Reports submitted while preparing for Compliance Audits.
12. The names of the Regional Entities where the Companies are registered, along with information that would indicate the involved Regional Entities.

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, January 25, 2019. Details about the Companies' operations, networks, and security should be treated and evaluated separately from the identity to

NERC Notice of Penalty

The Companies

January 25, 2019

Page 58

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 3-12 for three years from this filing date, January 25, 2019. 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. Completion of mitigation of the violations in this case;
2. Verification of mitigation completion;
3. Compliance monitoring of the Companies to ensure sustainability of the improvements described in this Notice of Penalty; and
4. Remediation of any subsequent violations discovered through compliance monitoring by the Regions or the Companies' improved self-monitoring.

The Companies should be less vulnerable to attempted attacks following these activities. After three years, disclosure of the identity of the Companies 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 the REs and the Companies, included as Attachment 1;
2. The Companies' mitigation activities to address the CIP-002-5.1 through CIP-011-2 violations, included as Attachment 2;
3. The Companies' Mitigation Plan, designated as [REDACTED], to address the CIP-014-2 violation, included as Attachment 3;
4. Record documents for the violation of CIP-002-5.1 R1 included as Attachment 4:
 - A. The Companies' Self-Report [REDACTED];
 - B. The Companies' Self-Report [REDACTED];
 - C. The Companies' Self-Report [REDACTED];
 - D. The Companies' Self-Report [REDACTED];
5. Record documents for the violation of CIP-003-3 R4, included as Attachment 5:
 - A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED];
6. Record documents for the violation of CIP-003-3 R6, included as Attachment 6:
 - A. Audit Summary [REDACTED]

NERC Notice of Penalty

The Companies

January 25, 2019

Page 59

- B. The Companies' Self-Report [REDACTED]
 - C. The Companies' Self-Report [REDACTED];
 - D. The Companies' Self-Report [REDACTED];
 - E. The Companies' Self-Report [REDACTED];
 - F. The Companies' Self-Report [REDACTED];
7. Record documents for the violation of CIP-004-3a R2, included as Attachment 7:
- A. The Companies' Self-Report [REDACTED];
8. Record documents for the violation of CIP-004-6 R2, included as Attachment 8:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
9. Record documents for the violation of CIP-004-3a R3, included as Attachment 9:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Expansion of Scope Assessment [REDACTED]
10. Record documents for the violation of CIP-004-6 R3, included as Attachment 10:
- A. The Companies' Self-Report [REDACTED];
 - B. The Companies' Self-Report [REDACTED];
 - C. The Companies' Self-Report [REDACTED]
 - D. The Companies' Self-Report [REDACTED];
11. Record documents for the violation of CIP-004-3a R4.2, included as Attachment 11:
- A. Audit Summary [REDACTED]
 - B. The Companies' Self-Report [REDACTED];
 - C. The Companies' Self-Report [REDACTED]
 - D. The Companies' Self-Report [REDACTED]
 - E. The Companies' Expansion of Scope Assessment [REDACTED];
 - F. The Companies' Self-Report [REDACTED]
 - G. The Companies' Self-Report [REDACTED]
 - H. The Companies' Self-Report [REDACTED];

NERC Notice of Penalty
The Companies
January 25, 2019
Page 60

12. Record documents for the violation of CIP-004-6 R4, included as Attachment 12:

- A. The Companies' Self-Report [REDACTED]
- B. The Companies' Self-Report [REDACTED]
- C. The Companies' Self-Report [REDACTED]
- D. The Companies' Self-Report [REDACTED]
- E. The Companies' Self-Report [REDACTED]
- F. The Companies' Self-Report [REDACTED]
- G. The Companies' Self-Report [REDACTED]

13. Record documents for the violation of CIP-004-6 R5, included as Attachment 13:

- A. The Companies' Self-Report [REDACTED]
- B. The Companies' Self-Report [REDACTED]
- C. The Companies' Self-Report [REDACTED]
- D. The Companies' Self-Report [REDACTED]
- E. The Companies' Self-Report [REDACTED]
- F. The Companies' Self-Report [REDACTED]
- G. The Companies' Self-Report [REDACTED]
- H. The Companies' Self-Report [REDACTED]
- I. The Companies' Self-Report [REDACTED]

14. Record documents for the violation of CIP-005-3a R1, included as Attachment 14:

- A. The Companies' Self-Report [REDACTED]
- B. The Companies' Self-Report [REDACTED]
- C. The Companies' Self-Report [REDACTED]
- D. The Companies' Self-Report [REDACTED]
- E. The Companies' Self-Report [REDACTED]
- F. The Companies' Self-Report [REDACTED]

15. Record documents for the violation of CIP-005-5 R1, included as Attachment 15:

- A. Audit Summary [REDACTED]
- B. The Companies' Self-Report [REDACTED]

NERC Notice of Penalty
The Companies
January 25, 2019
Page 61

- C. The Companies' Self-Report [REDACTED]
- D. The Companies' Self-Report [REDACTED]

16. Record documents for the violation of CIP-005-3a R2.1, R2.2, R2.4 included as Attachment 16:

- A. The Companies' Self-Report [REDACTED]
- B. The Companies' Self-Report [REDACTED]
- C. The Companies' Self-Report [REDACTED]

17. Record documents for the violation of CIP-005-5 R2 included as Attachment 17:

- A. The Companies' Self-Report [REDACTED]
- B. The Companies' Self-Report [REDACTED]
- C. The Companies' Self-Report [REDACTED]
- D. The Companies' Self-Report [REDACTED]
- E. Audit Summary [REDACTED]
- F. The Companies' Self-Report [REDACTED]

18. Record documents for the violation of CIP-006-3c R1 included as Attachment 18:

- A. The Companies' Self-Report [REDACTED]
- B. The Companies' Self-Report [REDACTED]
- C. The Companies' Self-Report [REDACTED]
- D. The Companies' Self-Report [REDACTED]
- E. The Companies' Self-Report [REDACTED]
- F. The Companies' Self-Report [REDACTED]
- G. Audit Summary [REDACTED]
- H. The Companies' Self-Report [REDACTED]
- I. The Companies' Self-Report [REDACTED]
- J. The Companies' Self-Report [REDACTED]
- K. The Companies' Self-Report [REDACTED]
- L. The Companies' Self-Report [REDACTED]

19. Record documents for the violation of CIP-006-6 R1 included as Attachment 19:

- A. The Companies' Self-Report [REDACTED]

NERC Notice of Penalty

The Companies

January 25, 2019

Page 62

- B. The Companies' Self-Report [REDACTED];
 - C. The Companies' Self-Report [REDACTED]
 - D. The Companies' Self-Report [REDACTED];
20. Record documents for the violation of CIP-006-3c R2.2 included as Attachment 20:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
21. Record documents for the violation of CIP-006-6 R2 included as Attachment 21:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
 - C. Audit Summary [REDACTED]
 - D. The Companies' Self-Report [REDACTED]
 - E. The Companies' Self-Report [REDACTED]
 - F. The Companies' Self-Report [REDACTED]
 - G. The Companies' Self-Report [REDACTED]
 - H. The Companies' Self-Report [REDACTED]
22. Record documents for the violation of CIP-006-3c R4 included as Attachment 22:
- A. The Companies' Self-Report [REDACTED]
23. Record documents for the violation of CIP-006-3c R5 included as Attachment 23:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
 - C. The Companies' Self-Report [REDACTED]
 - D. The Companies' Self-Report [REDACTED]
 - E. The Companies' Self-Report [REDACTED]
24. Record documents for the violation of CIP-007-3a R1.1 included as Attachment 24:
- A. Audit Summary [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
 - C. The Companies' Self-Report [REDACTED]
 - D. The Companies' Self-Report [REDACTED]

NERC Notice of Penalty
The Companies
January 25, 2019
Page 63

- E. The Companies' Self-Report [REDACTED]
25. Record documents for the violation of CIP-007-6 R1 included as Attachment 25:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
 - C. The Companies' Self-Report [REDACTED]
26. Record documents for the violation of CIP-007-6 R2 included as Attachment 26:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
 - C. The Companies' Self-Report [REDACTED]
 - D. The Companies' Self-Report [REDACTED]
 - E. The Companies' Self-Report [REDACTED]
 - F. The Companies' Self-Report [REDACTED]
 - G. The Companies' Self-Report [REDACTED]
 - H. The Companies' Self-Report [REDACTED]
27. Record documents for the violation of CIP-007-3a R3 included as Attachment 27:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
28. Record documents for the violation of CIP-007-6 R3 included as Attachment 28:
- A. The Companies' Self-Report [REDACTED]
29. Record documents for the violation of CIP-007-6 R4 included as Attachment 29:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
 - C. The Companies' Self-Report [REDACTED]
 - D. The Companies' Self-Report [REDACTED]
 - E. Audit Summary [REDACTED]
30. Record documents for the violation of CIP-007-3a R5 included as Attachment 30:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED]

NERC Notice of Penalty
The Companies
January 25, 2019
Page 64

C. The Companies' Self-Report [REDACTED]

D. The Companies' Self-Report [REDACTED];

31. Record documents for the violation of CIP-007-6 R5 included as Attachment 31:

A. The Companies' Self-Report [REDACTED]

B. The Companies' Self-Report [REDACTED]

C. The Companies' Self-Report [REDACTED]

D. The Companies' Self-Report [REDACTED]

E. The Companies' Self-Report [REDACTED]

F. The Companies' Self-Report [REDACTED]

32. Record documents for the violation of CIP-007-3a R6 included as Attachment 32:

A. Audit Summary [REDACTED]

33. Record documents for the violation of CIP-007-3a R7 included as Attachment 33:

A. The Companies' Self-Report [REDACTED]

34. Record documents for the violation of CIP-007-3a R8 included as Attachment 34:

A. The Companies' Self-Report [REDACTED]

35. Record documents for the violation of CIP-007-3a R9 included as Attachment 35:

A. The Companies' Self-Report [REDACTED]

36. Record documents for the violation of CIP-009-6 R1 included as Attachment 36:

A. The Companies' Self-Report [REDACTED]

B. The Companies' Self-Report [REDACTED]

37. Record Documents for the violation of CIP-009-6 R2

A. The Companies' Self-Report [REDACTED]

B. The Companies' Self-Report [REDACTED]

38. Record documents for the violation of CIP-009-6 R3 included as Attachment 38:

A. The Companies' Self-Report [REDACTED]

B. The Companies' Self-Report [REDACTED]

C. The Companies' Self-Report [REDACTED]

NERC Notice of Penalty
The Companies
January 25, 2019
Page 65

39. Record documents for the violation of CIP-010-2 R1 included as Attachment 39:

- A. Audit Summary [REDACTED]
- B. The Companies' Self-Report [REDACTED]
- C. The Companies' Self-Report [REDACTED]
- D. The Companies' Self-Report [REDACTED]
- E. Audit Summary [REDACTED]
- F. The Companies' Self-Report [REDACTED]
- G. The Companies' Self-Report [REDACTED]
- H. The Companies' Self-Report [REDACTED]
- I. The Companies' Self-Report [REDACTED]
- J. The Companies' Self-Report [REDACTED]
- K. Audit Summary [REDACTED]
- L. The Companies' Self-Report [REDACTED]
- M. The Companies' Self-Report [REDACTED]
- N. The Companies' Self-Report [REDACTED]
- O. The Companies' Self-Report [REDACTED]
- P. The Companies' Self-Report [REDACTED]

40. Record documents for the violation of CIP-010-2 R2 included as Attachment 40:

- A. Audit Summary [REDACTED]
- B. The Companies' Self-Report [REDACTED]
- C. The Companies' Self-Report [REDACTED]
- D. The Companies' Self-Report [REDACTED]
- E. The Companies' Self-Report [REDACTED]
- F. The Companies' Self-Report [REDACTED]

41. Record documents for the violation of CIP-010-2 R3 included as Attachment 41:

- A. The Companies' Self-Report [REDACTED]
- B. Audit Summary [REDACTED]
- C. The Companies' Self-Report [REDACTED]

NERC Notice of Penalty

The Companies

January 25, 2019

Page 66

- D. The Companies' Self-Report [REDACTED]
 - E. The Companies' Self-Report [REDACTED]
 - F. The Companies' Self-Report [REDACTED]
42. Record documents for the violation of CIP-010-2 R4 included as Attachment 42:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
43. Record documents for the violation of CIP-011-2 R1 included as Attachment 43:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
 - C. The Companies' Self-Report [REDACTED]
 - D. The Companies' Self-Report [REDACTED]
 - E. The Companies' Self-Report [REDACTED]
 - F. The Companies' Self-Report [REDACTED]
44. Record documents for the violation of CIP-011-2 R2 included as Attachment 44:
- A. Audit Summary [REDACTED]
 - B. The Companies' Self-Report [REDACTED]
 - C. The Companies' Self-Report [REDACTED]
45. Record documents for the violation of CIP-014-2 R1 included as Attachment 45:
- A. The Companies' Self-Report [REDACTED]
 - B. The Companies' Certification of Mitigation Plan Completion.

NERC Notice of Penalty

The Companies

January 25, 2019

Page 67

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

| | |
|--|---|
| <p>Sônia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net</p> <p>Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net</p> <p>Alexander Kaplen* Associate Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile alexander.kaplen@nerc.net</p> | <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> |
|--|---|

NERC Notice of Penalty
The Companies
January 25, 2019
Page 68
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

Sônia C. Mendonça
Vice President, Deputy General Counsel, and Director of
Enforcement
Edwin G. Kichline
Senior Counsel and Director of
Enforcement Oversight
Alexander Kaplen
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
alexander.kaplen@nerc.net

Attachments

Attachment 1

Settlement Agreement by and between the REs and the Companies

SETTLEMENT AGREEMENT

AMONG

AND

I. INTRODUCTION

1. (collectively, the Regions), and enter into this Settlement Agreement (Agreement) to resolve Alleged Violations by of the below-referenced Reliability Standard Requirements.¹ The Regions and are each referred to as a “Party” and collectively as “Parties.”

| Reliability Standard | Requirement | Tracking No. | NERC Tracking No. | Entity |
|----------------------|-------------|--------------|-------------------|--------|
| CIP-002-5.1 | R1.2 | | | |
| CIP-002-5.1 | R1.2 | | | |
| CIP-002-5.1 | R1.2 | | | |
| CIP-002-5.1 | R1.2 | | | |
| CIP-003-3 | R4.2 | | | |
| CIP-003-3 | R6 | | | |

¹ This Agreement references the version of the Reliability Standard in effect at the time each Alleged Violation began. The Companies, however, committed to perform mitigating actions to comply with the most recent version of each Reliability Standard Requirement.



| | | | | |
|------------|----------------------|------------|------------|------------|
| CIP-003-3 | R6 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-003-3 | R6 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-003-3 | R6 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-3a | R2.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R2; P2.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-3a | R3.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R3; P3.5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R3; P3.5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-3a | R4.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-3a | R4.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-3a | R4.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R4; P4.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R4; P4.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R4; P4.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R4; P4.2, P4.3, P4.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R5; P5.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R5; P5.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R5; P5.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R5; P5.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R5; P5.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R5; P5.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-004-6 | R5; P5.2, P5.3, P5.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-1 | R1.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-3a | R1.4 | [REDACTED] | [REDACTED] | [REDACTED] |



| | | | | |
|------------|-------------------------|------------|------------|------------|
| CIP-005-3a | R1.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-3a | R1.5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-3a | R1.5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-3a | R1.5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-5 | R1; P1.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-5 | R1; P1.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-5 | R1; P1.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-5 | R1; P1.5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-3a | R2.1, R2.2, R2.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-3a | R2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-3a | R2.5.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-5 | R2; P2.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-5 | R2; P2.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-5 | R2; P2.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-5 | R2; P2.1, P2.2, P2.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-005-5 | R2; P2.1, P2.2, P2.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R1.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R1.5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R1.6.1, R1.6.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R1.6.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-6 | R1; P1.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-6 | R1; P1.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-6 | R1; P1.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-6 | R1; P1.8 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-6 | R2; P2.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |



| | | | | |
|------------|----------------------------|------------|------------|------------|
| CIP-006-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-006-3c | R5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R1.1, R1.2, R1.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R1.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R1.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-6 | R1; P1.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-6 | R2; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-6 | R2; P2.2, P2.3, P2.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R3.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-6 | R3; P3.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-6 | R4; P4.1, P4.2, P4.3, P4.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-6 | R4; P4.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R5.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R5.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R5.3.3 | [REDACTED] | [REDACTED] | [REDACTED] |



| | | | | |
|------------|--|------------|------------|---|
| CIP-007-3a | R5.2, R5.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-6 | R5; P5.1, P5.2, P5.3, P5.4, P5.5, P5.6, P5.7 | [REDACTED] | [REDACTED] | [REDACTED] [REDACTED] [REDACTED] |
| CIP-007-6 | R5; P5.2 | [REDACTED] | [REDACTED] | [REDACTED] [REDACTED] [REDACTED] |
| CIP-007-6 | R5; P5.6 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R6.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R7.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R8.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-007-3a | R9 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-009-6 | R1; P1.1, P1.2, P1.3, P1.4, P1.5 | [REDACTED] | [REDACTED] | [REDACTED] [REDACTED], [REDACTED] |
| CIP-009-6 | R2; P2.1; P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-009-6 | R3; P3.1, P3.1.1, P3.1.2, P3.1.3, P3.2, P3.2.1, P3.2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R1; P1.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R1; P1.1.1 | [REDACTED] | [REDACTED] | [REDACTED] [REDACTED] [REDACTED] |
| CIP-010-2 | R1; P1.1, P1.1.1, P1.1.4 | [REDACTED] | [REDACTED] | [REDACTED] [REDACTED] [REDACTED] |
| CIP-010-2 | R1; P1.1.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R1; P1.1.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R1; P1.1.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R1; P1.1.5 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R1; P1.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R1; P1.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R1; P1.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R1; P1.4.1, P1.4.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R1; P1.4.1, P1.4.2 | [REDACTED] | [REDACTED] | [REDACTED] [REDACTED] [REDACTED] |
| CIP-010-2 | R2; P2.1 | [REDACTED] | [REDACTED] | [REDACTED] |

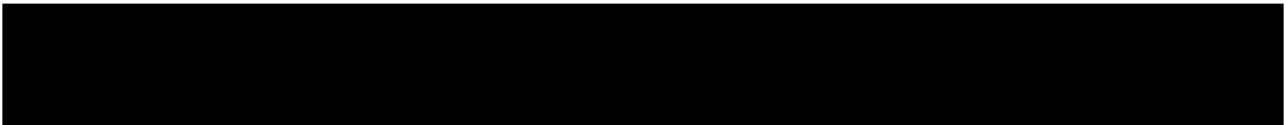
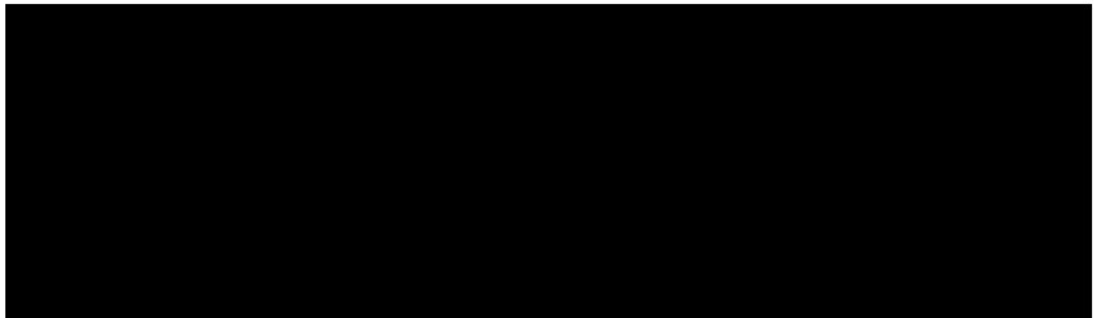


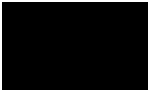
| | | | | |
|-----------|-------------------------|------------|------------|------------|
| CIP-010-2 | R2; P2.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R2; P2.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R2; P2.1 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R3; P3.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R3; P3.3 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R3; P3.1, P3.3, P3.4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-010-2 | R4 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-011-2 | R1; P1.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-011-2 | R1; P1.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-011-2 | R1; P1.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-011-2 | R1; P1.1, P1.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-011-2 | R2; P2.1, P2.2 | [REDACTED] | [REDACTED] | [REDACTED] |
| CIP-014-2 | R1 | [REDACTED] | [REDACTED] | [REDACTED] |

2. The Parties stipulate to the facts in this Agreement for the sole purpose of resolving the Alleged Violations. The [REDACTED] Companies admit that these facts constitute Alleged Violations of the above-referenced Reliability Standard Requirements.

II. OVERVIEW OF THE [REDACTED] COMPANIES

3. [REDACTED]





[REDACTED]

4. [REDACTED]

5. [REDACTED]

III. EXECUTIVE SUMMARY

Overview of Alleged Violations

6. This Settlement Agreement resolves 127 Alleged Violations of Critical Infrastructure Protection (“CIP”) Reliability Standards. These Alleged Violations include violations of CIP versions 3 and 5 and cover a total of 111 Self-Reports submitted from [REDACTED] through [REDACTED] and 16 Possible Violations discovered during the Regions’ [REDACTED] and [REDACTED] CIP Compliance Audits of [REDACTED]
7. During the Compliance Audits and subsequent enforcement processes, the Regions determined that [REDACTED] had serious, systemic security and compliance issues throughout its CIP compliance program covering multiple registrations. Of significant concern were the security risks around CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-010, and CIP-011. In these areas, many of the Alleged Violations involve long durations, multiple instances of noncompliance, and repeated failures to implement physical and cyber security protections, which illustrated [REDACTED] inability to implement effective corrective and preventative controls.³ Because the issues giving rise to the Alleged Violations were systemic

³ For CIP-003, [REDACTED] repeatedly failed to adhere to its change control and configuration management processes.

For CIP-004, [REDACTED] repeatedly granted electronic access rights to individuals who were not yet authorized to have access and failed to revoke access after individuals no longer required access. Often, the access incorrectly granted was to [REDACTED] of BES Cyber Systems and BES Cyber Assets.

and programmatic, the Regions considered the risk posed by the Alleged Violations and determined that the Alleged Violations, in the aggregate, posed a serious and substantial risk to the reliability of the Bulk Electric System (BES).⁴

8. The Alleged Violations resolved in this Settlement Agreement were rooted in cultural issues that allowed the Alleged Violations to occur and continue over an extended period of time, and upon identification, to not be properly addressed to ensure the CIP program was effective and sustainable. These issues materialized and were apparent through the following contributing causes of the Alleged Violations: (a) lack of management engagement, support, and accountability relating to the CIP compliance program;⁵ (b) disassociation of compliance and security that resulted in a deficient program and program documents, lack of implementation, and ineffective oversight and training; (c) organizational silos in the form of lack of communication between management levels within ██████ which contributed to a lack of awareness of the state of security and compliance; and (d) organizational silos across business units, which resulted in confusion regarding expectations and ownership of tasks and poor asset and configuration management practices. As discussed below, ██████ is addressing these programmatic issues through a comprehensive mitigation strategy, which the Regions will verify and

For CIP-005, ██████ repeatedly failed to identify and protect non-critical Cyber Assets within its Electronic Security Perimeter (ESP) for durations that spanned more than one year.

For CIP-006, ██████ repeatedly failed to properly provision physical access authorization requests. ██████ also failed to immediately review unauthorized access attempts to Physical Security Perimeters (PSPs) and failed to continuously monitor physical access at access points to PSPs.

For CIP-007, ██████ repeatedly failed to adhere to its cyber security test procedures when installing new Critical Cyber Assets. ██████ also failed to monitor vendor security patches and vulnerability notifications and repeatedly failed to timely assess and implement applicable patches.

For CIP-010, ██████ repeatedly failed to accurately document and track changes that deviate from existing baseline configurations dating back to the implementation date for CIP-010-2 on July 1, 2016.

For CIP-011, ██████ repeatedly failed to identify all BES Cyber System Information and securely handle it in accordance with the documented program.

⁴ While it is important to understand the overall risk given the nature of the Alleged Violations and contributing causes, the Regions also analyzed the potential risk for each Alleged Violation. Regarding individual risk determinations, of the 127 Alleged Violations, 13 posed a serious and substantial risk, 62 posed a moderate risk, and 52 posed a minimal risk.

⁵ As an example, ██████ failed to establish a single group that had ownership, accountability, resources, and authority to oversee ██████ CIP program. Additionally, ██████ staff lacked adequate resources, which led to an overreliance on contractors to perform CIP functions, which resulted in a lack of CIP knowledge among ██████ personnel.

validate through multiple measures.

Overview of Mitigation and Engagement with the Regions

9. [REDACTED] has committed to holistically reevaluate, redesign, and restructure its entire CIP compliance program, and implement measures to ensure its compliance program is both effective and sustainable. To that end, [REDACTED] committed to a mitigation approach that focuses on each compliance and security program area at issue in this Settlement, and for each area, [REDACTED] will: (a) engage business units and operational personnel to help revise and restructure its overarching enterprise-wide CIP program; (b) ensure the business unit processes and procedures meet the overarching program requirements; and (c) implement the new processes and procedures, including providing relevant training.
10. Additionally, to help ensure the effectiveness and sustainability of the CIP compliance and security program, [REDACTED] has committed to a number of additional measures relating to enhancing its centralized CIP oversight department, which acts as the central quality authority for [REDACTED] CIP program, including: (a) increased senior leadership involvement and oversight; (b) creating a centralized CIP oversight department and restructuring roles within that department to focus on areas such as Standards, Enterprise Oversight, Enterprise CIP Tools, compliance metrics, and regulatory interaction;⁶ (c) conducting industry surveys and benchmark discussions to help develop best practices relating to security and compliance practices; and (d) continuing its effort to develop an in-house NERC CIP program talent development program.
11. [REDACTED] has also committed to implement measures to support and assist its staff in implementing the CIP compliance program, including, for example: (a) investing over [REDACTED] in enterprise-wide tools relating to [REDACTED] [REDACTED] (b) adding additional resources to help manage compliance efforts; (c) instituting annual compliance drills; and (d) creating three levels of training (oversight training, awareness training for all staff, and performance training for staff implementing the security and compliance tasks).
12. The Regions note that [REDACTED] has recently made substantial efforts to be transparent and responsive and has made significant adjustments to the program. [REDACTED] has engaged with the Regions during the enforcement process [REDACTED] [REDACTED] for the purpose of holistically evaluating and improving [REDACTED] overall security posture. This has allowed [REDACTED] to gain a better understanding of its compliance program and the changes necessary to address the underlying issues to implement a sustainable CIP program. In addition to focusing

⁶ [REDACTED] has added additional resources to its centralized CIP oversight department, an expected [REDACTED] annual labor increase.



on cultural and enterprise-wide changes necessary to improve its program, [REDACTED], is focusing on key high risk areas in its CIP program, such as patching, to identify deficiencies and strategies for improving [REDACTED] security posture and program sustainability.

13. Due to the systemic nature of the violations and causes contributing to the violations, the Regions anticipate that [REDACTED] will identify additional instances of noncompliance while completing mitigation. While [REDACTED] comprehensive mitigation, which the Regions are very closely monitoring, should address any compliance issues that [REDACTED] identifies during mitigation, [REDACTED] is required to report these instances to the Regions upon identification, and the Regions will verify that the instance are mitigated.
14. The Regions are not awarding any above and beyond credit for these actions because, in light of [REDACTED] compliance history and the nature of the current Alleged Violations, these actions are necessary for [REDACTED] to implement an effective and sustainable CIP compliance program.

Background Regarding [REDACTED] Compliance History

15. As background, the Regions have filed [REDACTED] Notices of Penalty against [REDACTED] to resolve [REDACTED] distinct packages of Alleged Violations of CIP Standards within the last [REDACTED] years.
16. First, in [REDACTED], the Regions filed [REDACTED] full Notices of Penalty covering all [REDACTED] Registrations in [REDACTED] against [REDACTED] resolving a combined [REDACTED] violations of the CIP Standards, including [REDACTED] serious risk violations, and levied a combined monetary penalty of [REDACTED]. The violations included a combination of Self-Reports and violations identified during Compliance Audits conducted in [REDACTED]. The Regions determined that [REDACTED] suffered from compliance silos and ineffective internal controls. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
17. Second in [REDACTED], the Regions filed [REDACTED] Notices of Penalty that resolved a combined [REDACTED] violations of the CIP Standards and levied a combined monetary penalty of [REDACTED]. The violations include a combination of Self-Reports and violations identified during a Compliance Audit conducted in [REDACTED]. These [REDACTED] violations did not contain any serious risk violations. Many of the [REDACTED] violations in these [REDACTED] Notices of Penalty were repeats of the violations filed in [REDACTED] and were aggravated for [REDACTED] compliance history. The Regions determined that [REDACTED] CIP compliance program continued to be hindered by compliance silos and that there was disassociation between compliance and security at [REDACTED]



18. The prior violations involve many of the same Standards and Requirements and similar conduct as the violations at issue in the current CIP Settlement Agreement. While [REDACTED] completed mitigation for the prior violations, [REDACTED] failed to resolve the underlying cultural issues, which prevented [REDACTED] from implementing a sustainable CIP program and permitted the Alleged Violations to occur.

Overview of Penalty and Sanctions

19. Since the beginning of mandatory compliance with the CIP Standards, [REDACTED] has struggled to implement an effective and sustainable CIP compliance program. [REDACTED] significant and programmatic CIP compliance and security issues were exacerbated by cultural issues stemming from its lack of management involvement. The multi-year duration of [REDACTED] serious risk issues combined with [REDACTED] absence of corrective and preventative controls put the BES at serious risk for a long duration. This, together with [REDACTED] compliance history and [REDACTED] overall potential impact to the BES, warrant a significant penalty and sanctions.

IV. ADJUSTMENT FACTORS

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

Lack of Management Involvement

21. The Regions considered that [REDACTED] management passively accepted [REDACTED] prior violations by creating and allowing a culture to exist that permitted these systemic problems to continue for more than five years. This is evidenced by the number of violations, the duration of the violations, the risk posed by the violations, and the number of repeat violations. Therefore, the Regions considered [REDACTED] lack of management involvement as an aggravating factor for penalty purposes.

Compliance History

22. The Regions considered whether the facts of these 127 Alleged Violations constitute repetitive infractions. [REDACTED] has prior violations of CIP-003 R5 and R6, CIP-004 R3 and R4, CIP-005 R1, CIP-006 R1 and R5, CIP-006 R5, and CIP-007 R1, R2, R3, R5, and R6.⁷ In accordance with the Commission's directive that the North American Electric Reliability Corporation ("NERC") and the Regions consider a violator's corporate affiliates when assessing repeat violations, the Regions considered the fact that many of the Alleged Violations resolved within this Agreement involve some or all of [REDACTED] [REDACTED] has a history of Alleged Violations for many of the same Standards and Requirements that are at

⁷ See Attachment 1 for full compliance history.

issue in the current CIP Settlement Agreement, and the current Alleged Violations involve similar conduct as the prior violations. Therefore, the Regions considered [REDACTED] compliance history as an aggravating factor for penalty purposes.

V. PENALTY AND SANCTION

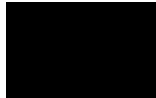
23. Based upon the foregoing, [REDACTED] shall pay a monetary penalty of \$10,000,000.00 in total to the Regions. [REDACTED] shall pay \$10,000,000.00 to [REDACTED] and [REDACTED] shall divide that penalty amount [REDACTED] based on the relative net energy for load (“NEL”) for each Region⁸ [REDACTED]
[REDACTED] [REDACTED] [REDACTED]
24. In addition to the monetary penalty, the Regions are imposing three non-monetary sanctions on [REDACTED]. First, [REDACTED] Chief Executive Officer (CEO) must sign the Settlement Agreement as a direct sanction. Given that [REDACTED] ineffective management oversight and engagement is a contributing cause of the Alleged Violations, it is critical that executive leadership at [REDACTED] support and be fully engaged in [REDACTED] CIP compliance program to ensure its success in the future.
25. Second, [REDACTED] must provide quarterly reports to its Board of Directors and the Regions until the Regions determine that such reporting is no longer necessary. The Regions will work with [REDACTED] to determine the proper format and content of the quarterly reports, but the reports will generally include at least metrics relating to, on a going-forward basis, all identified potential noncompliance and near misses; the root cause of each instance; mitigation progress for each instance; the status of all [REDACTED] enterprise-wide improvements; and any potential or missed deadlines and the identified obstacle or cause.
26. Third, the Regions will perform increased compliance monitoring to monitor higher-risk areas across [REDACTED] program and verify the accuracy of the content within [REDACTED] dashboard. This will include periodic monitoring, including targeted CIP audits, spot checks, and/or self-certifications.
27. [REDACTED] 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. [REDACTED] will notify NERC if it does not timely receive the payment from [REDACTED]
28. If [REDACTED] fails to timely remit the monetary penalty payment to [REDACTED] interest will

⁸ NEL is published in NERC’s annual business plan and budget and is used as a method to prorate fee assessments. The calculation used for this Agreement is based on the NERC 2017 budget, which indicates the following NEL values in the ERO: [REDACTED] [REDACTED] For the purposes of penalty calculation in this Agreement, the NEL values correspond to weighted penalties of [REDACTED] to [REDACTED]

commence to accrue on the outstanding balance, pursuant to 18 C.F.R. § 35.19a (a)(2)(iii), on the earlier of (a) the 31st day after the date on the invoice issued by [REDACTED] to [REDACTED] for the monetary penalty payment or (b) the 51st day after the Agreement is approved by the Commission or operation of law.

VI. ADDITIONAL TERMS

29. 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.
30. [REDACTED] 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 [REDACTED] 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 Alleged Violations and the terms provided for in this Agreement.
31. This Agreement binds the Parties upon execution, and may only be altered or 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.
32. [REDACTED] 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.
33. [REDACTED] consents to [REDACTED] 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.



34. [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 the Regions enters into this Agreement in express reliance on the representations contained herein, as well as any other representations or information provided by [REDACTED] to the Regions during any [REDACTED] interaction with the Regions relating to the subject matter of this Agreement. Any errors or omissions made in good faith by the parties shall not invalidate this agreement.
35. Upon execution of this Agreement, the Parties stipulate that each Possible Violation addressed herein constitutes an Alleged Violation. The Parties further stipulate that all required, applicable information listed in Section 5.3 of the CMEP is included within this Agreement.
36. 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.
37. 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.
38. The Agreement may be signed in counterparts.
39. This Agreement is executed in duplicate, each of which so executed shall be deemed to be an original.

[SIGNATURE PAGE TO FOLLOW]⁹

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

⁹ An electronic version of this executed document shall have the same force and effect as the original.

ATTACHMENT A

I. ALLEGED VIOLATIONS

A. CIP-002-5.1a R1 ([REDACTED])

40. CIP-002-5 ensures the identification and categorization of BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.
41. CIP-002-5.1a provides:
- 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 Cranking 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.
- 1.1.** Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;
- 1.2.** Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and
- 1.3.** Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

Description of Alleged Violation for [REDACTED]

42. On September 8, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-002-5.1a R1.2. *See* Self-Report, **Attachment 2a.** [REDACTED] failed to maintain an accurate BES Cyber System (BCS) inventory.
43. On January 16, 2017, during an ad hoc comparison review between [REDACTED] BCS

inventory and inventory database device list, [REDACTED] discovered that two [REDACTED] [REDACTED] located in different [REDACTED] were not identified in its BCS inventory.

44. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on November 30, 2017, when [REDACTED] revised its BCS inventory to include the [REDACTED].

Description of Alleged Violation for [REDACTED]

45. On December 6, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] was in violation of CIP-002-5.1a R1.2. *See* Self-Report, **Attachment 2b**. [REDACTED] failed to maintain an accurate BCS inventory.
46. On June 26, 2017, [REDACTED] discovered that it had not identified [REDACTED] medium impact BCS and [REDACTED] associated BES Cyber Assets (BCAs) within a [REDACTED] placed into service on March 17, 2017.
47. The Alleged Violation started on [REDACTED], when [REDACTED] failed to identify the BCS and associated BCAs that comprised the BCS, and ended on June 26, 2017, when [REDACTED] revised its BCS inventory to include the associated BCAs.

Description of Alleged Violation for [REDACTED]

48. On December 6, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] was in violation of CIP-002-5.1a R1.2. *See* Self-Report, **Attachment 2c**. [REDACTED] failed to maintain an accurate BCS inventory.
49. On [REDACTED] [REDACTED] commissioned a [REDACTED] and placed a BCS comprising of [REDACTED] [REDACTED] into service. However, on July 20, 2017, [REDACTED] discovered that it had not identified the [REDACTED] in the BCS inventory.
50. The Alleged Violation began on [REDACTED], when [REDACTED] commissioned the [REDACTED] without identifying the [REDACTED] as BCAs, and ended on July 21, 2017, when [REDACTED] updated its BCS inventory to include the [REDACTED].

Description of Alleged Violation for [REDACTED]

51. On December 11, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-002-5.1a R1.2. *See* Self-Report, **Attachment 2d**. [REDACTED] failed to maintain an accurate BCS inventory.
52. On September 19, 2017, during a 15-month review of BCAs, [REDACTED] discovered that its BCA inventory list included an outdated cranking path associated with a Blackstart Resource. In July 2015, [REDACTED] made a change to its [REDACTED] Restoration Plan, [REDACTED]. The formation of the [REDACTED] changed

[REDACTED]

the cranking path associated with the Blackstart Resource; however, [REDACTED] failed to update its BCS inventory to reflect the change in the cranking path.

53. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on September 21, 2017, when [REDACTED] updated its BCS inventory to reflect the change in the correct cranking path.

Aggregate Contributing Causes of CIP-002-5.1a R1 Alleged Violations

54. The primary cause of the CIP-002-5.1a R1 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] BCS categorization process had broad categorization choices, which increased the risk of human error when selecting categories, and there was no secondary review in place to minimize human error. Additionally, during the implementation of new Cyber Assets (CAs) in different [REDACTED] [REDACTED] did not implement consistent processes across its [REDACTED] functional groups. Additional training, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violations.

Aggregate Risk Statement for CIP-002-5.1a R1 Alleged Violations

55. The Regions determined that the Alleged Violations posed an aggregate moderate risk¹⁰ to the reliability of the Bulk Power System based on the following factors.¹¹ [REDACTED] failure to develop an accurate BCS inventory increased the risk that [REDACTED] would not implement security controls on applicable CAs that comprised the BCSs. However, [REDACTED] did implement the following protective measures. For all four CIP-002-5.1a R1 Alleged Violations, the subject CAs were protected inside a 24/7 monitored PSP, which could only be accessed with proper credentials. For two¹² of these four Alleged Violations, the CAs were also afforded all other required CIP security controls. For the two¹³ remaining Alleged Violations, the CAs were also isolated from the corporate networks and had no Internet connectivity. [REDACTED] attested that no cyber security incidents or events were detected for the duration of the Alleged Violations.

¹⁰ Alleged Violation [REDACTED], individually, posed a moderate risk to the reliability of the BPS, and [REDACTED] individually, posed a minimal risk.

¹¹ CIP-002-5.1a R1 has a VRF of “High” pursuant to the VRF Matrix. According to the VSL Matrix, these Alleged Violations warranted a “Lower” VSL.

¹² [REDACTED]

¹³ [REDACTED]



Mitigating Actions for CIP-002-5.1a R1 Alleged Violations

56. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-002-5.1a R1 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
57. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED]
[REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
58. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

B. CIP-003-3 R4 [REDACTED]

59. CIP-003-3 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.
60. CIP-003-3 R4 provides:
 - R4.** Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
 - R4.1.** The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster

recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

Description of Alleged Violation for [REDACTED]

61. On September 22, 2015, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-003-3 R4.2.¹⁴ See Self-Report, **Attachment 3a**. [REDACTED] failed to classify documentation as CCA information. On November 24, 2015, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-003-3 R4.1.¹⁵ See Self-Report, **Attachment 3b**. This Alleged Violation involves two instances where [REDACTED] failed to protect Critical Cyber Asset (CCA) information in accordance with its information protection program.
62. In the first instance, on April 30, 2015, while updating one-line diagrams at [REDACTED] Critical Asset [REDACTED] [REDACTED] identified [REDACTED] one-line diagrams without the appropriate NERC CIP classification markings. [REDACTED] discovered that on May 1, 2011, during a network design project, a former employee removed the classification markings from the one-line diagrams.
63. This instance started on May 1, 2011, when [REDACTED] failed to mark CCA information, and ended on May 5, 2015, when [REDACTED] appropriately classified the CCA information.
64. In the second instance, [REDACTED] [REDACTED] employees were granted “read-only” access rights to CCA information maintained in an information file repository. On August 11, 2015, [REDACTED] discovered that the file repository was misconfigured and allowed all [REDACTED] employees access to the CCA information. On August 3, 2015, [REDACTED] performed a file share conversion and configured [REDACTED] CCA information file shares to “read-only” access. However, when [REDACTED] configured the file shares, the changes cascaded through subdirectories and removed “deny” permissions on subfolders. [REDACTED] discovered the issue while processing an Information Technology (IT)

¹⁴ The Alleged Violation was self-reported under R4.1; however, the Regions determined that R4.2 is the applicable Requirement.

¹⁵ This self-reported noncompliance was assigned NERC Tracking Number [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on April 15, 2016.

[REDACTED]

trouble ticket. A user reported a file share permission issue, and while investigating, the technical staff discovered the incorrect file share security permissions allowing unauthorized access to CCA information.

65. This instance started on August 3, 2015, when unauthorized personnel received access to CCA information, and ended on August 11, 2015, when [REDACTED] modified the access permissions, thereby effectively revoking access rights to CCA information for unauthorized personnel.
66. The contributing causes for the CIP-003-3 R4 Alleged Violation were insufficient training and a deficient process. Additional training was necessary to ensure that applicable IT personnel were made aware that the file share contained sensitive CIP information that must be protected. Additionally, the process did not include clear requirements for marking one-line drawings as CCA information. For example, the [REDACTED] separate one-line communication diagrams for the [REDACTED] [REDACTED] were replaced with a “template drawing.” The NERC CIP stamp classification was left off the template; therefore, the classification was not included on the new one-line diagrams.
67. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the Bulk Power System based on the following factors.¹⁶ The risk posed by [REDACTED] failure to identify and protect CCA information was providing the opportunity for unauthorized access to sensitive information. Notwithstanding, the risk was mitigated because the duration of the instances of noncompliance was only five and eight days, respectively. Additionally, regarding the first instance, most of the unauthorized personnel who received access to the CCA information were not aware of the change in their access rights. Regarding the second instance, the risk was mitigated because [REDACTED] stored the documents containing CCA information within a secure information repository, and only authorized personnel had access to the documents.

Mitigation Actions for CIP-003-3 R4 Alleged Violations

68. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-003-3 R4 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
69. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED]: (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal

¹⁶ CIP-003-3 R4 has a VRF of “Lower” pursuant to the VRF Matrix. According to the VSL Matrix, this noncompliance warranted a “Severe” VSL.

[REDACTED]

controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

70. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

C. CIP-003-3 R6 [REDACTED]
[REDACTED]

71. CIP-003-3 ensures that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

72. CIP-003-3 R6 provides:

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

Description of Alleged Violation for [REDACTED]

73. During a Compliance Audit conducted [REDACTED], the Regions determined that [REDACTED] as a [REDACTED] [REDACTED] and [REDACTED] was in violation of CIP-003-3 R6. See PV Audit Summary, **Attachment 4a**. This Alleged Violation involves three instances where [REDACTED] failed to follow its documented change control and configuration management process.

74. In all three instances, software upgrades were deployed on a single Critical Cyber Asset (CCA) in the production environment without first being tested in accordance

with [REDACTED] change control process. [REDACTED] automated configuration management tool detected the changes and alerted appropriate personnel.

75. The Alleged Violation started on September 3, 2015, when, in the first instance, the software update was deployed without adherence to [REDACTED] change control and configuration management process, and ended on July 31, 2018, when [REDACTED] conducted a vulnerability assessment and confirmed that the implementation of the service pack did not impact security controls.

Description of Alleged Violation for [REDACTED]

76. On June 30, 2016, July 15, 2016, and August 10, 2016, [REDACTED] submitted three Self-Reports, on behalf of [REDACTED] [REDACTED] to [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] it was in violation of CIP-003-3 R6. *See* Self-Reports, **Attachments 4b, 4c,¹⁷ and 4d.¹⁸** The Self-Reports include a total of four instances where [REDACTED] failed to adhere to its change control and configuration management process.
77. In the first instance, on April 10, 2016, [REDACTED] was alerted of an unauthorized change to a CCA by its [REDACTED] tool. [REDACTED] discovered that on April 4, 2016, with an authorized change request, a [REDACTED] employee installed a service pack to a single CCA. [REDACTED] vendor recommended the installation of the service pack because there was a prior hardware failure on the associated CCA. However, the [REDACTED] employee was unaware that the service pack included a firmware change, which had not been tested prior to implementation in the production environment because it was not included as part of the authorized change request.
78. In the second instance, on June 4, 2016, [REDACTED] was alerted of an unauthorized change to a non-CCA by its [REDACTED] tool. [REDACTED] discovered that on June 3, 2016, a [REDACTED] employee installed software on one non-CCA without an authorized change request. Thus, the software was not tested prior to implementation in the production environment.
79. In the third instance, on May 2, 2016, during a process improvement exercise, [REDACTED] discovered unauthorized changes to multiple BES Cyber Assets (BCAs). Specifically, on March 8, 2016, a [REDACTED] employee issued a change management ticket through its automated workflow software to implement a software change to [REDACTED] Cyber Assets (CAs). On March 10, 2016, the [REDACTED] employee implemented the

¹⁷ This self-reported noncompliance was assigned NERC Tracking Number [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on December 20, 2016.

¹⁸ This self-reported noncompliance was never assigned a NERC Tracking Number. Instead, it was assigned an internal tracking number [REDACTED], which was administratively dismissed and consolidated with [REDACTED] on August 18, 2016.

software change on all [REDACTED] CAs; however, the employee failed to mark [REDACTED] CAs as NERC CIP assets. As a result, the software was not tested prior to implementation for those [REDACTED] CAs.

80. In the fourth instance, on May 22, 2016, [REDACTED] was alerted of an unauthorized change to one CCA by its [REDACTED] tool. On May 21, 2016, with an authorized change request, a [REDACTED] employee implemented an anti-virus software upgrade to [REDACTED] BCAs. [REDACTED] determined that during the implementation of the anti-virus software upgrade, the [REDACTED] employee implemented an additional software upgrade to one CCA, which was not included in the authorized change request. Consequently, the additional software upgrade was not tested prior to implementation in the production environment.
81. The Alleged Violation started on April 4, 2016, when, in the first instance, the software update was deployed without adherence to [REDACTED] change control and configuration management process, and ended on July 20, 2016, when [REDACTED] completed testing for the last instance.

Description of Alleged Violation for [REDACTED]

82. On August 31, 2016, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-003-3 R6. *See* Self-Report, **Attachment 4e**. [REDACTED] failed to adhere to its change control and configuration management process.
83. On March 10, 2016, during an internal review of CIP compliance data in preparation for an upcoming [REDACTED] compliance audit, [REDACTED] discovered that on May 13, 2015, [REDACTED] performed [REDACTED] upgrades on [REDACTED] of its [REDACTED] but failed to maintain the necessary documentation throughout the change control and configuration management process.
84. The Alleged Violation started on May 13, 2015, when [REDACTED] implemented a service pack to a CCA in the production environment without first testing it, and ended on March 31, 2017, when [REDACTED] conducted a vulnerability assessment and confirmed that the implementation of the service pack did not impact security controls.

Description of Alleged Violation for [REDACTED]

85. On August 8, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-003-3 R6. *See* Self-Report, **Attachment 4f**. [REDACTED] failed to adhere to its change control and configuration management process.
86. [REDACTED] discovered the noncompliance on September 12, 2016, during an annual CIP-002 walk-down of a [REDACTED]. Prior to the walk-down, [REDACTED] identified an

[REDACTED]

inconsistency between CCAs identified in the physical inventory list and the asset database. [REDACTED] confirmed the inconsistency during the walk-down and discovered that on May 20, 2015, it replaced a failed [REDACTED] at the [REDACTED], but did not update its asset database as required by its documented change control and configuration management process.

87. The Alleged Violation started on May 20, 2015, when [REDACTED] replaced a [REDACTED] without updating the asset database, and ended on October 31, 2016, when [REDACTED] updated the asset database and verified [REDACTED] baseline parameters.

Aggregate Contributing Causes of CIP-003-3 R6 Alleged Violations

88. The primary cause of the CIP-003-3 R6 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the change control and configuration management process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] process did not clearly define the roles and responsibilities of [REDACTED] personnel. Additionally, change requests and workflows did not require a validation process before final authorization. Additional training, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violations.

Aggregate Risk Statement for CIP-003-3 R6 Alleged Violations

89. The Regions determined that the Alleged Violations posed an aggregate serious and substantial risk¹⁹ to the reliability of the Bulk Power System based on the following factors.²⁰ The risk posed by [REDACTED] failure to adhere to its change control and configuration management process was providing the opportunity for the introduction of vulnerabilities to CCAs. However, [REDACTED] did implement the following protective measures. For six of the nine instances, [REDACTED] [REDACTED] tool detected the unauthorized changes and notified the appropriate personnel in a timely manner, which prompted investigations. [REDACTED] had logging and monitoring in place, which should have alerted [REDACTED] of any detected cyber security incidents or events.
90. Despite these protective measures, the aggregate risk remains serious and substantial based on several factors. From May 13, 2015 through June 3, 2016, [REDACTED] had [REDACTED] instances where it implemented changes to [REDACTED] CCAs without first testing. The Regions determined that [REDACTED] had serious, systemic security and

¹⁹ Alleged Violations [REDACTED] individually, posed a moderate risk to the reliability of the BPS, and [REDACTED] individually, posed a minimal risk.

²⁰ CIP-003-3 R6 has a VRF of “Lower” pursuant to the VRF Matrix. According to the VSL Matrix, this noncompliance warranted a “Severe” VSL.

[REDACTED]

compliance issues across its [REDACTED] functional groups, which required [REDACTED] to overhaul its entire CIP compliance program. Because of this, the risk for continued noncompliance and compromise to BCSs and CAs dramatically increased. Due to the weaknesses in [REDACTED] CIP compliance program, the Regions anticipate that [REDACTED] will identify additional instances of noncompliance while completing mitigation, which [REDACTED] will report to the Regions. Notwithstanding, [REDACTED] comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that [REDACTED] reports.

Mitigation Actions for CIP-003-3 R6 Alleged Violations

91. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-003-3 R6 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
92. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED]
[REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
93. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

D. CIP-004-3a R2 [REDACTED]

94. CIP-004-3a protects Critical Cyber Assets by requiring that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of Personnel Risk Assessment, training, and security awareness.



95. CIP-004-3a R2 provides in relevant part:

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

Description of Alleged Violation and Risk Assessment for [REDACTED]

96. On August 5, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED] they were in violation of CIP-004-3a R2.1. *See* Self-Report, **Attachment 5a**. [REDACTED] failed to maintain annual cyber security training for [REDACTED] of its employees with authorized electronic access and/or physical access to Critical Cyber Assets (CCAs).

97. On February 4, 2016, in preparation for implementing a new access management tool, [REDACTED] reviewed the list of employees and contractors with authorized electronic and physical access to [REDACTED] CCAs. [REDACTED] identified [REDACTED] employees who did not have current cyber security training. On February 17, 2016, [REDACTED] conducted another analysis prior to the deployment of the new tool and identified [REDACTED] additional employees who did not have training. [REDACTED] of the involved employees had physical access and [REDACTED] had electronic access (none had both types of access). Instead of immediately revoking the employees' access rights, [REDACTED] communicated to all



applicable personnel the requirement to perform the current training no later than February 29, 2016, or their access would be revoked and not carried over to the new tool.

98. On February 29, 2016, [REDACTED] deployed its new access management tool; however, [REDACTED] employees still had not completed the training. The [REDACTED] employees who did not complete the training had their access revoked on February 5, 2016, February 17, 2016, February 26, 2016, and March 1, 2016.
99. The primary cause of the CIP-004-3a R2 Alleged Violation was lack of managerial oversight. Contributing causes were an ineffective access management software, a deficient process, and lack of internal controls. The access management software was outdated and did not always generate reminder alerts to personnel when training was due or automatically revoke access once the employee's training expired. As a result, personnel were required to manually review and verify employees' access rights; however, [REDACTED] manual process was not documented. [REDACTED] lacked internal controls to ensure that personnel adhered to [REDACTED] manual process to review and verify personnel training expiration dates and revoke access rights upon expiration. Proper managerial oversight should have identified the undocumented manual review and verification process and implemented stronger internal controls to help ensure that the process was sufficient and followed.
100. The Alleged Violation started on January 1, 2016, when the first individual's training expired, and ended on March 1, 2016, the last date that [REDACTED] revoked access rights of the individuals whose training expired.
101. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the Bulk Power System based on the following factors.²¹ The risk posed by [REDACTED] failure to ensure that all personnel having access to CCAs were trained was providing the opportunity for misuse of CCAs, CCA information, and delay in recovering or re-establishing CCAs. The risk was mitigated because the [REDACTED] individuals identified for failing to complete the mandatory annual training had timely completed the previous annual training. Additionally, all [REDACTED] individuals had current Personnel Risk Assessments on file, and logging and alerting was in place at all access points into Physical Security Perimeters.

²¹ CIP-004-3a R2 has a VRF of "Lower" pursuant to the VRF Matrix. According to the VSL Matrix, this noncompliance warranted a "Severe" VSL.



Mitigation Actions for CIP-004-3a R2 Alleged Violation

102. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-004-3a R2 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
103. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED]: (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
104. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

E. CIP-004-6 R2 [REDACTED]

105. The purpose of CIP-004-6 is to minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (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.
106. CIP-004-6 R2 provides in relevant part:
 - 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.



P2.2. 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.

P2.3. Require completion of the training specified in Part 2.1 at least once every 15 calendar months.

Description of Alleged Violation for [REDACTED]

107. On April 20, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-004-6 R2; P2.2. *See* Self-Report, **Attachment 6a.** [REDACTED] did not provide cyber security training to an individual prior to granting electronic access to protected Cyber Assets (CAs).
108. On March 8, 2017, the [REDACTED] used a batch method to upload multiple individuals and associated business roles to the [REDACTED] [REDACTED], which aligned with each individual's authorized electronic access permissions. However, this batch method did not validate Personnel Risk Assessments (PRAs) and training prerequisites, and once the names and business roles were uploaded, all access permissions became available to the individuals. One individual in the batch did not satisfy the training prerequisites, yet [REDACTED] granted the individual "read-only" access to the passwords for [REDACTED] [REDACTED] and [REDACTED] [REDACTED] cyber assets with a medium impact rating.
109. On March 31, 2017, a project team identified the unauthorized access to the passwords while preparing for a May release and reconciling training data with role requirements in [REDACTED] [REDACTED]. On March 31, 2017, [REDACTED] revoked access for that individual.
110. The Alleged Violation started on March 8, 2017, when [REDACTED] granted electronic access to the passwords prior to training, and ended on March 31, 2017, when [REDACTED] revoked the individual's access rights.

Description of Alleged Violation for [REDACTED]

111. On June 19, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-004-6 R2; P2.3.²² *See* Self-Report, **Attachment 6b.** [REDACTED] failed to maintain training for one employee with access to applicable CAs.

²² The Alleged Violation was self-reported under CIP-004-6 R5, P5.2; however, the Regions determined that CIP-004-6 R2, P2.3 is the applicable Standard and Requirement.



112. On June 8, 2016, a [REDACTED] team member submitted a request in the [REDACTED] to revoke an individual's physical badge access rights to [REDACTED] NERC CIP locations because the individual's cyber security training was about to expire. However, the [REDACTED] member should have submitted the request to remove the individual's access for [REDACTED] locations. On April 28, 2017, during the 2017 first quarterly review, [REDACTED] discovered that it had not removed the individual's access to the [REDACTED] location and that the individual's cyber security training had expired on September 28, 2016.
113. The Alleged Violation started on September 28, 2016, when the individual's training expired, and ended on April 28, 2017, when [REDACTED] revoked the individual's access rights.

Aggregate Root Causes of CIP-004-6 R2 Alleged Violations

114. The primary cause of the CIP-004-6 R2 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. In the first Alleged Violation, [REDACTED] cyber security training process did not clearly define individual roles and responsibilities. For instance, the [REDACTED] team had a documented job aid, which explained how to use the batch process, but it did not clearly state that it would not check prerequisites when adding roles to workers. In addition, the job aid did not direct the [REDACTED] team to validate prerequisites manually before using the batch process to add roles to workers. Further, [REDACTED] did not have any controls in place to prevent training from lapsing. Regarding the second Alleged Violation, [REDACTED] had an undocumented manual process to validate access removal in its badging system, which produced inconsistent results in the application of the process. Further, the [REDACTED] team member did not follow the quarterly review process for identifying, researching, and resolving discrepancies, and there was no requirement for a secondary review to ensure that the process was followed. While [REDACTED] removed access in the [REDACTED] it did not actually remove access in the end system, and as a result, the individual still had access to the [REDACTED] location. Additional training, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violations.



Aggregate Risk Statement for CIP-004-6 R2 Alleged Violations

115. The Regions determined that the Alleged Violations posed a moderate risk²³ to the reliability of the Bulk Power System.²⁴ The risk posed by [REDACTED] failure to ensure that all personnel having access to high and medium impact CAs are trained was providing the opportunity for misuse of such CAs or associated asset information, or could delay in recovering or re-establishing such CAs. The risk was mitigated because, for both Alleged Violations, the individuals were current [REDACTED] employees and had current PRAs on file, thus reducing the likelihood that the individuals would use the access in a way as to compromise CCAs. [REDACTED] confirmed that the employees did not attempt to access the password repository prior to completing cyber security training.

Mitigation Actions for CIP-004-6 R2 Alleged Violations

116. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-004-6 R2 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
117. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED]: (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
118. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED]

²³ Alleged Violation [REDACTED], individually, posed a moderate risk to the reliability of the BPS, and [REDACTED], individually, posed a minimal risk.

²⁴ According to the CIP-004-6 Table of Compliance Elements, this noncompliance warrants a “Lower” VRF and a “Lower” VSL.

completion of the Mitigation Activities and promptly report its successful completion to NERC.

F. CIP-004-3a R3 [REDACTED]

119. CIP-004-3a protects Critical Cyber Assets by requiring that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of Personnel Risk Assessment, training, and security awareness.

120. CIP-004-3a R3 provides in relevant part:

R3. Personnel Risk Assessment — The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

....

Description of Alleged Violation and Risk Assessment for [REDACTED]

121. On July 21, 2015, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-004-3a R3.2. *See* Self-Report, **Attachment 7a.** [REDACTED] failed to timely update three employees' Personnel Risk Assessments (PRAs).

122. On March 31, 2015, while performing a review of employees' physical and

electronic access rights, [REDACTED] discovered that it failed to perform a seven-year PRA update for one employee who had physical and electronic access to Critical Cyber Assets (CCAs). Because [REDACTED] completed the employee's previous PRA on November 12, 2007, it was required to perform the seven-year PRA update by November 12, 2014.

123. Each month, [REDACTED] [REDACTED] was responsible for validating individuals with access to CCAs had current PRAs on file and had completed the required CIP training. In doing so, the [REDACTED] generated a report by exporting the employee access information from its training system and manually reviewed the report. On November 13, 2014, the [REDACTED] generated and reviewed the report but failed to identify the one employee who should have had his PRA updated on or before November 12, 2014. On March 31, 2015, [REDACTED] discovered the oversight and initiated a PRA update, which was completed on April 1, 2015.
124. On December 22, 2015, [REDACTED] submitted an expansion of scope assessment to [REDACTED] on behalf of [REDACTED] [REDACTED] with two additional instances of expired PRAs. *See* Expansion of Scope, **Attachment 7b**. On August 6, 2015, during an internal control review of its training data, [REDACTED] discovered that two employees with electronic access to CCAs did not have updated PRAs and immediately revoked their access rights. The employees' existing PRAs expired on May 19, 2015, and May 26, 2015. [REDACTED] updated the PRAs on August 10, 2015, and August 11, 2015, respectively.
125. The primary cause was lack of managerial oversight. Contributing causes included a deficient process and weak internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. Although personnel manually reviewed employees' PRAs, this manual review and verification process was not documented, which increased the risk for errors. In the first instance, while performing the manual review, an error was made when generating the list. Additionally, [REDACTED] lacked internal controls to ensure that PRAs were properly reviewed and verified.
126. The Alleged Violation started on November 13, 2014, the date the earliest PRA expired, and ended on August 6, 2015, the date the last PRA was renewed.
127. The Regions determined that the Alleged Violation posed a minimal risk to the

reliability of the Bulk Power System based on the following factors.²⁵ The risk posed by [REDACTED] failure to ensure that all PRAs were current was providing the opportunity for untrusted or unreliable individuals to physically access CCAs, resulting in the misuse or compromise of CCAs. This risk was mitigated because the three employees were current employees of [REDACTED] were properly given access to CCAs, and were current on cyber security training, thus reducing the likelihood that the individuals would use the access in a way as to compromise CCAs.

Mitigation Actions for CIP-004-3a R3 Alleged Violations

128. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-004-3a R3 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
129. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
130. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

G. CIP-004-6 R3 [REDACTED]

131. CIP-004-6 reduces the risk of compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring

²⁵ CIP-004-3a R3.2 has a VRF of “Lower” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Moderate” VSL.

an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

132. CIP-004-6 R3 provides in relevant part:

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-6 Table R3 – Personnel Risk Assessment Program.

....

P3.5. Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.

Description of Alleged Violation for [REDACTED]

133. On August 31, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] was in violation of CIP-004-6 R3; P3.5.²⁶ See Self-Report, **Attachment 8a.** [REDACTED] failed to timely update a Personnel Risk Assessment (PRA) for one contractor with unescorted physical access to BES Cyber Systems (BCSs).
134. On June 29, 2016, a [REDACTED] manager requested approval for one contractor to be granted unescorted physical access to [REDACTED] Physical Security Perimeters (PSPs). Because [REDACTED] utilized the contractor's services in 2015, the contractor completed cyber security training in 2015 and 2016, and had a PRA on file. On June 30, 2016, [REDACTED] verified the contractor was current on cyber security training and had a PRA on file and granted the access requested. However, [REDACTED] did not review the date that the contractor's PRA was completed, which was June 30, 2009.
135. On July 5, 2016, [REDACTED] conducted a prescheduled bi-weekly meeting to evaluate expiring cyber security training and PRAs. [REDACTED] entered the date the contractor's PRA was completed; however, [REDACTED] PRA verification system was configured so that it would not validate PRAs that were set to expire within 45 days. As a result, the PRA verification system did not validate the contractor's PRA, and [REDACTED] discovered that the PRA expired on June 30, 2016, the same day it granted the contractor's physical access rights. [REDACTED] revoked the contractor's physical access

²⁶ The Alleged Violation was self-reported under CIP-004-3a R3.2; however, the Regions determined that CIP-004-6 R3.5 is the applicable Standard and Requirement because of the start date of the noncompliance.



on July 5, 2016, and initiated the process for an updated PRA.

136. The Alleged Violation started on July 1, 2016, the day following the expiration of the PRA, and ended on July 5, 2016, when [REDACTED] revoked the contractor's physical access rights.

Description of Alleged Violation for [REDACTED]

137. On May 22, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-004-6 R3; P3.5. *See* Self-Report, **Attachment 8b**. Also, on April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-004-6 R3; P3.5.²⁷ *See* Self-Report, **Attachment 8c**. On January 23, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation of CIP-004-6 R4; P3.5.²⁸ *See* Self-Report, **Attachment 8d**. This Alleged Violation includes three instances where [REDACTED] failed to ensure individuals with authorized electronic and/or physical access to BCSs had current PRAs.
138. In the first instance, the [REDACTED] [REDACTED] was responsible for monitoring and revoking individuals' access rights, including creating lists of workers who had CIP access, sending reminders to those workers and managers whose PRAs were about to expire, and revoking access upon the expiration of PRAs. On February 20, 2017, a deviation from this process occurred when the [REDACTED] [REDACTED] project team, using lists provided by the [REDACTED], began sending out notifications to workers whose PRAs were going to expire in preparation for a change in classification to the [REDACTED] application. On February 20, 2017, March 13, 2017, and April 3, 2017, [REDACTED] sent emails to employees whose PRAs were close to expiring. However, during an April 24-25, 2017 quarterly CIP access review, the [REDACTED] discovered that two employees' PRAs expired on April 16, 2017. The employees each had access to over [REDACTED] BCAs.
139. In the second instance, during a Cyber Asset categorization review on January 5, 2017, [REDACTED] discovered that it had not identified [REDACTED] [REDACTED] as EACMSs. As a result, [REDACTED] failed to ensure that all individuals with authorized

²⁷ This noncompliance was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-004-6 R3.5 is the applicable Standard and Requirement.

²⁸ This noncompliance was self-reported as CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-004-6 R3.5 is the applicable Standard and Requirement.

[REDACTED]

electronic and unescorted physical access to the EACMSs had a current PRA.

140. This instance affected a total of [REDACTED]
141. In the third instance, as part of an extent of condition assessment on November 15, 2017, [REDACTED] determined that it had not identified [REDACTED] servers as EACMSs. As a result, [REDACTED] failed to ensure that all individuals with authorized electronic and unescorted physical access to the EACMS servers had a current PRA.
142. This instance affected a total of [REDACTED]
143. The Alleged Violation started July 1, 2016, when, in the second and third instances, the Standard became mandatory and, and will end on [REDACTED], when [REDACTED] committed to complete its Mitigation Plan.

Aggregate Contributing Causes of CIP-004-6 R3

144. The primary cause of the CIP-004-6 R3 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. Regarding the first instance where PRAs of two employees expired, [REDACTED] access management process did not clearly define the roles and responsibilities of assignments between the [REDACTED] and [REDACTED], which contributed to human performance issues in completing their assignments. Although the [REDACTED] was responsible for monitoring and revoking employee access rights, they believed the [REDACTED] project team was temporarily taking over those responsibilities during the implementation phase of the application change to the [REDACTED]. For the second and third instances, [REDACTED] personnel lacked adequate training to identify in-scope EACMSs. Additional training, along with clearer designations and instructions of individual and team tasks could have prevented these Alleged Violations.
145. The Regions determined that the Alleged Violations posed an aggregate moderate risk²⁹ to the reliability of the Bulk Power System based on the following factors.³⁰

²⁹ Alleged Violation [REDACTED], individually, posed a moderate risk to the reliability of the BPS, and [REDACTED], individually, posed a minimal risk.

³⁰ CIP-004-6 R3 has a VRF of “Medium” pursuant to the CIP-004-6 Table of Compliance Elements. According to the VSL Matrix, this noncompliance warranted a “Lower” VSL.

[REDACTED]

The risk posed by [REDACTED] failure to ensure that all PRAs were current was providing the opportunity for untrusted or unreliable individuals to physically access BCSs, resulting in the misuse or compromise of such systems. Regarding the first instances, the risk was mitigated because the two individuals had completed cyber security training and had a valid PRA at the time physical access rights were granted, and were properly given access to BCSs, thus reducing the likelihood that the individuals would use the access in a way as to compromise BCSs. Additionally, the duration of the Alleged Violations were 4 and 9 days, respectively. Regarding the second and third instances, although [REDACTED] did not provide evidence of valid PRAs for all individuals with authorized electronic or physical access to the subject EACMSs, these EACMSs are inside PSPs. Thus, the current PRAs of all individuals with authorized access to identified EACMSs not subject to this Alleged Violation would have applied to all EACMSs. However, because the subject EACMSs were not identified and documented as EACMSs, [REDACTED] failed to follow its process and ensure that all individuals with access to these EACMSs had current PRAs.

Mitigation Actions for CIP-004-6 R3 Alleged Violations

146. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-004-6 R3 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
147. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
148. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED]

completion of the Mitigation Activities and promptly report its successful completion to NERC.

H. CIP-004-3a R4 [REDACTED]

149. CIP-004 protects Critical Cyber Assets by requiring that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of Personnel Risk Assessment, training, and security awareness.

150. CIP-004-3a R4 provides:

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

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

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

Description of Alleged Violation for [REDACTED]

151. During a Compliance Audit conducted [REDACTED], the Regions determined that [REDACTED] as a [REDACTED] [REDACTED] and [REDACTED] was in violation of CIP-004-3a R4.2. *See* PV Summary, **Attachment 9a**. [REDACTED] failed to timely revoke a former employee's electronic access rights.

152. From a sample of terminations, the Regions identified one instance where [REDACTED] failed to revoke a former employee's electronic access to Critical Cyber Assets (CCAs) within 24 hours after the employee was terminated for cause. On April 2, 2015, a [REDACTED] manager initiated a change management ticket to revoke an employee's access effective April 3, 2015; however, the manager did not mark the ticket as a for-cause termination. On April 3, 2015, [REDACTED] terminated the employee for cause, which initiated the 24-hour revocation requirement. Additionally, upon termination, the [REDACTED] manager did not notify the help desk of the employee

terminated for cause per internal processes so that the help desk could immediately revoke access.

153. The noncompliance started on April 4, 2015, when the former employee's access rights were required to be revoked, and ended on April 7, 2015, when [REDACTED] revoked the access rights.
154. On March 11, 2016, April 7, 2016, and June 15, 2016, [REDACTED] submitted three Self-Reports to [REDACTED] and on April 20, 2016, [REDACTED] as a [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED] submitted an expansion of scope to [REDACTED] stating that they discovered three additional CIP-004-3a R4.2 instances where access was not timely revoked. *See* Self-Reports and Expansion of Scope, **Attachments 9b**,³¹ **9c**,³² **9d**³³, and **9e**.³⁴
155. In the first instance, on October 28, 2015, a [REDACTED] contractor's employment ended, but the account manager did not follow [REDACTED] internal process of notifying the appropriate [REDACTED] personnel to revoke the contractor's physical badge access to CCAs within seven calendar days from date of termination. On December 29, 2015, [REDACTED] discovered that the former contractor's badge was still active, and [REDACTED] immediately deactivated the badge.
156. This instance of noncompliance started on November 5, 2015, when the former contractor's access rights were required to be revoked, and ended on December 29, 2015, when [REDACTED] revoked the access rights.
157. In the second instance, [REDACTED] policy required a 30-calendar-day break for contractors who had been on an assignment for 36 consecutive months, even when a contractor would return after the break on the same assignment. On December 1, 2015, [REDACTED] required a contractor to go on a 30-day absence. The contractor's manager failed to follow [REDACTED] internal process of completing the required change access request documentation to revoke the contractor's physical badge access. As a result, [REDACTED] failed to revoke the contractor's access within seven calendar days from date the contractor was put on a temporary break. [REDACTED] revoked the contractor's access on December 23, 2015.

³¹ This self-reported noncompliance was assigned NERC Tracking Number [REDACTED] but was later administratively dismissed and consolidated with [REDACTED]

³² This self-reported noncompliance was assigned NERC Tracking Number [REDACTED] but was later administratively dismissed and consolidated with [REDACTED]

³³ This self-reported noncompliance was assigned [REDACTED] Tracking Number [REDACTED] but was later administratively dismissed and consolidated with [REDACTED]

³⁴ [REDACTED] reported this noncompliance as an expansion of scope, but it was never assigned a NERC Tracking Number.



158. This instance of noncompliance started on December 8, 2015, when the former contractor's access rights were required to be revoked, and ended on December 23, 2015, when [REDACTED] revoked the access rights.
159. In the third instance, [REDACTED] failed to revoke access within seven calendar days for an employee who no longer required access to CCAs. On February 16, 2016, an employee submitted a badge access request to revoke access to NERC assets and to add, remove, and modify access to non-NERC assets. Due to system design limitations, the badge access system could not process NERC and non-NERC access requests or revocations on the same ticket, so [REDACTED] NERC access services team rejected the change ticket. However, the system failed to perform as expected and processed the request ticket as approved. Instead of removing access, the system granted the individual access. The request was in error because the individual was not authorized for access to the NERC assets. The [REDACTED] [REDACTED] received notification that the system granted access. The team notified the [REDACTED] to remove the unauthorized access.
160. This instance of noncompliance started on February 16, 2016, when the individual was granted unauthorized access, and ended the same day, when [REDACTED] revoked access.
161. In the fourth instance, on January 5, 2016, while performing its quarterly access review, a [REDACTED] manager discovered one employee who no longer needed access to CCAs, as of October 1, 2015. Therefore, [REDACTED] should have removed access on or before October 8, 2015. On January 5, 2016, the manager created a badge access request revocation ticket for both NERC and non-NERC access. The change request was authorized; however, the badge access system was not designed to process NERC and non-NERC access requests or revocations on the same ticket. Therefore, the system failed to revoke access as requested. On January 6, 2016, [REDACTED] discovered that the badge access system did not revoke the employee's access, alerted the appropriate personnel responsible for revoking such access, and requested that the access be immediately revoked. Instead of immediately revoking access, the employee created a reminder to complete the task later. The employee, however, did not revoke access until January 18, 2016.
162. This instance of noncompliance started on October 9, 2015, when the former employee's access rights were required to be revoked, and ended on January 18, 2016, when [REDACTED] revoked the access rights.

Description of Alleged Violation for [REDACTED]

163. On August 11, 2016, and September 2, 2016, [REDACTED] submitted two Self-Reports to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] [REDACTED] and [REDACTED] they were in violation of CIP-004-3a R4.2. *See* Self-Reports, **Attachments 9f and 9g**.³⁵ The Self-Reports include multiple instances where [REDACTED] failed to revoke employees' access within seven calendar days after access was no longer required.
164. In the first self-reported instance, on March 21, 2016, a [REDACTED] manager initiated an access revocation for an employee who was scheduled to voluntarily depart the company on April 1, 2016. Because the employee had electronic access to CCAs, the manager initiated the revocation request in the newly implemented automated access revocation tool. However, the request never became finalized because the manager inadvertently kept the request in draft form. On April 12, 2016, the [REDACTED] manager realized the mistake and finalized the revocation request. On April 13, 2016, upon reviewing the request, [REDACTED] discovered the untimely access revocation and immediately revoked the access.
165. The noncompliance started on April 8, 2016, when the former employee's electronic access rights were required to be revoked, and ended on April 13, 2016, when [REDACTED] revoked the access rights.
166. In the second self-reported instance, on April 14, 2016, during a review of an access revocation report generated from the new access management software, [REDACTED] discovered that on five different occasions, [REDACTED] did not timely revoke employees' access rights that were no longer needed. [REDACTED] discovered that employees improperly submitted access termination requests on March 1, 2016, March 10, 2016, April 1, 2016 (two), and April 4, 2016. Each of the employees was transferring within the company and had nonessential access for between four and 37 days. On April 15, 2016, [REDACTED] revoked access for the last of the five employees.
167. This instance of noncompliance started on March 8, 2016, when the first transferring employee's access rights were required to be revoked, and ended on April 15, 2016, when [REDACTED] revoked access rights for the last of all five employees.
168. In the third self-reported instance, on June 30, 2016, during its quarterly access review, [REDACTED] discovered that it had failed to timely revoke two employees'

³⁵ This self-reported noncompliance was never assigned a NERC Tracking Number. Instead, it was assigned an internal tracking number [REDACTED], which was administratively dismissed and consolidated with [REDACTED] on September 20, 2016.



authorized unescorted physical access to CCAs. On February 1, 2016, an employee transferred to a new position within the company, but [REDACTED] failed to revoke CCA access until July 1, 2016. Additionally, on May 31, 2016, [REDACTED] voluntarily terminated an employee, but the manager did not begin the access revocation process until June 9, 2016.

- 169. For the first individual, the noncompliance started on February 8, 2016, when the transferring employee's access rights were required to be revoked, and ended on July 1, 2016, when [REDACTED] revoked the employee's access rights. For the second individual, the noncompliance started on June 8, 2016, when the former employee's access rights were required to be revoked, and ended on June 9, 2016, when [REDACTED] revoked the employee's access rights.
- 170. Of the seven individuals in the second and third self-reported instances, two individuals had physical and electronic access, two individuals had only electronic access, and three individuals had only physical access.

Description of Alleged Violation for [REDACTED]

- 171. On September 12, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-004-3a R4.2.³⁶ See Self-Report, **Attachment 9h**. [REDACTED] did not revoke a contractor's physical access rights within seven calendar days from the date of termination.
- 172. On July 15, 2015, the contractor changed employers, but the contractor's employer did not notify [REDACTED]. On April 13, 2017, during a review of the physical access list, [REDACTED] discovered that the former contractor no longer required physical access and revoked the individual's physical access rights on the same day.
- 173. The scope of affected facilities included [REDACTED]
Affected Cyber Assets [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]. [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED], [REDACTED]
[REDACTED], [REDACTED] [REDACTED]
- 174. The Alleged Violation started on July 22, 2015, when [REDACTED] should have revoked the former contractor's physical access rights, and ended on April 13, 2017, when [REDACTED] revoked the physical access rights.

³⁶ The Alleged Violation was self-reported under CIP-004-6 R5.1; however, the Regions determined that CIP-004-3a R4.2 is the applicable Standard and Requirement because of the start date of the noncompliance.



Aggregate Contributing Causes of CIP-004-3a R4 Alleged Violations

175. The primary cause of the CIP-004-3a R4 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. For all instances, the process was complex, with multiple steps, which did not clearly define employee roles and responsibilities. For example, there was an unclear designation of NERC versus non-NERC access within the badge accessing system, which contributed to human performance issues in completing the access removal tasks. Additionally, [REDACTED] lacked internal controls to ensure sufficient training had been provided to the [REDACTED] employees and contractors. Additional training, along with clearer designations and instructions of individual and team tasks could have prevented these Alleged Violations.

Aggregate Risk Assessment for CIP-004-3a R4 Alleged Violations

176. The Regions determined that the Alleged Violations posed an aggregate moderate risk³⁷ to the reliability of the Bulk Power System based on the following factors.³⁸ The risk posed by [REDACTED] failure to timely revoke electronic and physical access to CCAs was providing the opportunity for personnel who should no longer have access to CCAs, to access CCAs. The risk was mitigated because, in all instances, all individuals had a business need for access when access was granted, were current on cyber security training, had current PRAs on file, and none attempted to access CCAs after they no longer needed such access. [REDACTED] provided training and security awareness to assist employees' identification of suspicious and/or malicious behavior. Therefore, had an employee noticed suspicious activity, the employee should have known the proper actions. Regarding the multiple instances of noncompliance included in the second Alleged Violation, six of the eight employees merely transitioned to new roles within [REDACTED]. Regarding the third Alleged Violation where [REDACTED] failed to timely revoke a contractor's physical access rights, the risk was mitigated because the former vendor employee did not have electronic access. [REDACTED] had cameras at each access point and confirmed that the individual did not access any Physical Security Perimeter for the duration of this Alleged Violation. Notwithstanding these mitigating measures, the aggregate risk was elevated because, between April 4, 2015, and June 8, 2016, a total of [REDACTED]

³⁷ All Alleged Violations, individually, posed a minimal risk to the reliability of the BPS.

³⁸ CIP-004-3a R4.2 has a VRF of "Lower" pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a "Severe" VSL.

individuals maintained access that was no longer required. Moreover, the last Alleged Violation, the former contractor's physical access rights were not revoked until almost 21 months after access was no longer needed.

Mitigation Actions for CIP-004-3a R4 Alleged Violations

177. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-004-3a R4 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
178. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
179. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

I. CIP-004-6 R4 [REDACTED]
[REDACTED]

180. CIP-004-6 reduces the risk of 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.
181. CIP-004-6 R4 provides:
- 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.

P4.1. Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

P4.1.1. Electronic access;

P4.1.2. Unescorted physical access into a Physical Security Perimeter; and

P4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

P4.2. Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.

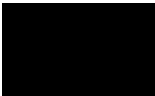
P4.3. For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.

P4.4. Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

Description of Alleged Violation for [REDACTED]

182. On February 28, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] [REDACTED] and [REDACTED] they were in violation of CIP-004-6 R4; P4.1. *See* Self-Report, **Attachment 10a.** [REDACTED] granted one individual unescorted physical access that was not needed.

183. On September 14, 2016, the [REDACTED] [REDACTED] received an approved request to add NERC badge access for an individual to multiple NERC CIP Physical Security Perimeters (PSPs). On [REDACTED], the [REDACTED] began the access provisioning process as requested. The member of [REDACTED] responsible for completing the access request was waiting to validate access in the Physical Access Control Systems (PACSs) to complete the request. Although the requested access permissions were granted, this [REDACTED] employee failed to complete and closeout this access request once the PACSs access verification was completed.



184. On September 20, 2016, the supervisor who submitted the initial approved access request realized that the individual did not need access to all of the locations included in the initial request and submitted a second approved request to remove a portion of the NERC badge access permissions. That same day, the [REDACTED] member completed the process and removed access that was not needed as indicated in the second approved access request.
185. On September 23, 2016, a different [REDACTED] employee noticed that the initial access request received on September 14, 2016 had not been completed in the system. The employee determined that the [REDACTED] had not granted all of the access requested and reprocessed the access request, thereby adding the access back that was removed from the second request. Later that day, the individual's supervisor identified the issue after receiving notification that the access permissions, which the [REDACTED] was supposed to remove, were granted. The supervisor immediately contacted a [REDACTED], who immediately removed the unnecessary access permissions in accordance with the second access request received on September 20, 2016.
186. [REDACTED] gave the individual unauthorized access to [REDACTED]
[REDACTED] and [REDACTED]
[REDACTED]
187. The noncompliance started on September 23, 2016, when [REDACTED] granted the employee unnecessary access permissions to the PACSs, and ended on September 23, 2016, when the [REDACTED] removed the employee's access permissions from the PACSs.

Description of Alleged Violation for [REDACTED]

188. On June 19, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-004-6 R4; P4.1. See Self-Report, **Attachment 10b**. [REDACTED] granted [REDACTED] individuals electronic access to CIP-protected information they did not need.
189. On March 20, 2017, an Information Technology (IT) compliance analyst started the transfer of files from a folder on a server to the [REDACTED] repository. During this process, the analyst noticed that the large amount of data [REDACTED] was attempting to transfer was creating a performance issue on the [REDACTED] site, which caused the analyst to stop the transfer before it was completed. On [REDACTED], the IT analyst submitted a work order to have the files restored



back to the server. However, the mechanism that [REDACTED] used to restore files and folders for this network attached storage (NAS) device restored the deleted folders with the same permissions as the parent folder. As a result, the new permissions from the parent folder provided additional personnel access to the NAS device.

190. On April 26, 2017, [REDACTED] determined that it granted unauthorized access. Upon further review, [REDACTED] identified [REDACTED] individuals with unauthorized access permissions.
191. This instance affected [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED]. On May 18, 2017, [REDACTED] restored the individuals' correct access permissions.
192. The noncompliance started on March 23, 2017, when [REDACTED] granted unauthorized access, and ended on May 18, 2017, when [REDACTED] revoked the unauthorized access.

Description of Alleged Violation for [REDACTED]

193. On September 8, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-004-6 R4; P4.1. See Self-Report, **Attachment 10c**. [REDACTED] granted one individual electronic access to its Energy Management System (EMS) without proper authorization.
194. On February 27 and 28, 2017, [REDACTED] [REDACTED] [REDACTED] were performing [REDACTED] tuning with assistance from a vendor. The vendor used an [REDACTED] engineer's keyboard and mouse to navigate through various [REDACTED] displays in order to instruct the [REDACTED] personnel on new functionality features for tuning [REDACTED] on the recently upgraded [REDACTED] platform. The vendor then entered data into the [REDACTED] for certain parameters for purposes of tuning [REDACTED]. However, [REDACTED] never granted the vendor authorized electronic access to perform these tasks. On March 30, 2017, [REDACTED] CIP program management was conducting compliance-related inquiries with staff when it discovered that the vendor's electronic access was unauthorized.
195. The Alleged Violation started on February 27, 2017, when [REDACTED] allowed the vendor unauthorized access to the [REDACTED], and ended on February 28, 2017, the last day the vendor accessed the [REDACTED].

Description of Alleged Violation for [REDACTED]

196. On November 27, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] and [REDACTED] they were in violation of CIP-004-6

[REDACTED]

R4; P4.1. *See* Self-Report, **Attachment 10d**.³⁹ [REDACTED] improperly granted one employee electronic access to BCSs and failed to remove physical access for six individuals in accordance with its access management program.

197. On April 10, 2017, [REDACTED] granted a new employee electronic access to a CIP password repository without utilizing the software system required by its documented access management program. On July 11, 2017, while performing a quarterly CIP access review, [REDACTED] discovered this access discrepancy, which affected [REDACTED] containing [REDACTED] and [REDACTED]. On July 12, 2017, [REDACTED] followed its program requirements for provisioning the individual proper access.
198. Additionally, during an extent-of-condition review, [REDACTED] discovered five additional individuals with unescorted physical access for which it did not verify authorization records. Upon further review, [REDACTED] determined that access for these five individuals needed to be revoked on November 22, 2016, January 4, 2017, January 19, 2017, February 7, 2017, and February 17, 2017, but [REDACTED] did not properly revoke such access. [REDACTED] did not discover these discrepancies during subsequent quarterly reviews.
199. The Alleged Violation started on November 22, 2016, when [REDACTED] should have revoked the first individual's physical access, and ended August 11, 2017, when [REDACTED] revoked access for the last individual involved.

Description of Alleged Violation for [REDACTED]

200. On January 22, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-004-6 R4; P4.1 - P4.4.⁴⁰ *See* Self-Report, **Attachment 10e**. On April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-004-6 R4; P4.2; P4.3; and P4.4.⁴¹ *See* Self-Report, **Attachment 10f**. On January 23, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on

³⁹ This Self-Report stemmed from an extent of condition review under [REDACTED] (CIP-004-6 R2; P2.3) in which [REDACTED] identified five additional workers whose physical access rights had not been removed from [REDACTED] PSPs. However, the Regions determined that CIP-004-6 R4; P4.1 is the applicable Standard and Requirement and consolidated the noncompliance with [REDACTED]

⁴⁰ The Alleged Violation was self-reported under CIP-004-6 R4, P4.1; however, the Regions determined that P4.2 is also an applicable sub-part.

⁴¹ This noncompliance was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-004-6 R4 is the applicable Standard and Requirement.

██████████

behalf of ██████████ ██████████ ██████████ ██████████ stating that, as ██████████ they were in violation of CIP-004-6 R4; P4.2; P4.3; and P4.4.⁴² See Self-Report, **Attachment 10g**. This Alleged Violation involves three instances where ██████████ failed to conduct the required access verification reviews required by CIP-004-6 R4.

201. In the first instance, during a quarterly review of ██████████ electronic access list on November 13, 2017, ██████████ discovered that on October 28, 2016, it incorrectly assigned one employee to a system shared user account on an EACMS server, which affected ██████████ EACMS devices. During multiple subsequent quarterly verification reviews, ██████████ missed the inconsistency between the individual's authorization records and actual authorization.
202. In the second instance, during a CA categorization review on January 5, 2017, ██████████ discovered that it had not identified ██████████ as EACMSs. As a result, ██████████ failed to verify access authorization records (P4.2); electronic access user account groups, role categories, and specific associated privileges were correct and necessary (P4.3); and that designated storage for BES Cyber System Information were correct and necessary for performing work functions (P4.4).
203. This instance affected a total of ██████████ associated with ██████████ ██████████.
204. In the third instance, as part of an extent of condition assessment on November 15, 2017, ██████████ discovered that it had not identified ██████████ servers as EACMSs. As a result, ██████████ failed to verify access authorization records (P4.2); electronic access user account groups, role categories, and specific associated privileges were correct and necessary (P4.3); and that designated storage for BES Cyber System Information were correct and necessary for performing work functions (P4.4).
205. This instance affected a total of ██████████ ██████████ and ██████████ ██████████ ██████████.
206. The Alleged Violation started July 1, 2016, when the Standard became mandatory and enforceable, and will end on ██████████, when ██████████ committed to complete its Mitigation Plan.

⁴²This noncompliance was self-reported as CIP-002-5.1a R1 and assigned NERC Tracking Number ██████████. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-004-6 R4 is the applicable Standard and Requirement.



Aggregate Contributing Causes of CIP-004-6 R4

207. The primary cause of the CIP-006-6 R4 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. For the first Alleged Violation, [REDACTED] personnel were unaware that the software system used to revoke access did not automatically revoke access, and personnel did not adhere to the verification process to ensure that access had been revoked. Additionally, [REDACTED] process did not include instructions for access requests that were on hold or remained open pending the completion of additional tasks. Regarding the second Alleged Violation where the compliance analyst granted [REDACTED] individuals electronic access to CIP-protected information they did not need, the analyst was unaware that restoring the folder would give it the permissions of the parent folder. Additionally, [REDACTED] did not have controls in place to ensure that folders would be restored with the correct permissions. Regarding the fourth Alleged Violation where an employee was assigned to the wrong user account in the access management system, the process did not require, and there was no internal control to verify, that the user was assigned to the correct user account. For the fifth Alleged Violation where [REDACTED] failed to identify EACMSs, [REDACTED] personnel lacked adequate training to identify in-scope EACMSs. Additional training, along with clearer instructions of the process could have helped prevent these Alleged Violations.

Aggregate Risk Assessment for CIP-004-6 R4

208. This Regions determined that the Alleged Violations posed an aggregate serious and substantial risk⁴³ to the reliability of the Bulk Power System (BPS).⁴⁴ The risk posed by these Alleged Violation was providing the opportunity for personnel who should not have access to BCSs, to access such systems. However, for all Alleged Violations, [REDACTED] had physical and electronic access logging and monitoring for incident detection and response. Regarding the first, fourth, and first instance of the fifth Alleged Violations, all eight individuals with unauthorized access or access to CIP-protected information that was not needed were [REDACTED] employees, were properly granted access to BCSs, were current on cyber security training, and had a current PRA on file when access was granted thus reducing the likelihood that the individuals would use the unauthorized access in a way that would compromise the

⁴³ Alleged Violations [REDACTED], individually, posed a moderate risk to the reliability of the BPS, and [REDACTED], individually, posed a minimal risk.

⁴⁴ CIP-004-6 R4 has a VRF of “Medium” pursuant to the CIP-004-6 Table of Compliance Elements. According to the VSL Matrix, this noncompliance warranted a “Severe” VSL.

[REDACTED]

BPS. In the third Alleged Violation where [REDACTED] granted one vendor employee electronic access to its EMS without proper authorization, [REDACTED] retained the vendor's services to assist in AGC tuning, and the vendor performed all tasks in the presence of [REDACTED] staff.

209. Notwithstanding, the aggregate risk remains serious and substantial based on several factors. Between September 23, 2016 and November 9, 2017 (less than 14 months), at least [REDACTED] individuals had unauthorized access to BCSs. The Regions determined that [REDACTED] had serious, systemic security and compliance issues across its [REDACTED] functional groups, which required [REDACTED] to overhaul its entire CIP compliance program. Because of this, risk for continued noncompliance and compromise to BCSs and CAs dramatically increased. Due to the weaknesses in [REDACTED] CIP compliance program, the Regions anticipate that [REDACTED] will identify additional instances of noncompliance while completing mitigation, which [REDACTED] will report to the Regions. Notwithstanding, [REDACTED] comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that [REDACTED] reports.

Mitigation Actions for CIP-004-6 R4 Alleged Violations

210. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-004-6 R4 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
211. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.



212. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

J. CIP-004-6 R5 [REDACTED]
[REDACTED]

213. CIP-004-6 reduces the risk of 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.

214. CIP-004-6 R5 provides:

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.

P5.1. 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).

P5.2. For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

P5.3. For termination actions, revoke the individual’s access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.

P5.4. For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.

P5.5. 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 Alleged Violation for [REDACTED]

- 215. On September 12, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] was in violation of CIP-004-6 R5; P5.1.⁴⁵ See Self-Report, **Attachment 11a.** [REDACTED] did not timely revoke eight individuals' unescorted physical access to a control center Physical Security Perimeter (PSP) within 24 hours from termination.
- 216. In November of 2016, the facilities management service provider for [REDACTED] sent contract termination letters to three contract companies, affecting an aggregate of eight employees, with terminations effective December 31, 2016. On June 16, 2017, during a quarterly review of [REDACTED] physical access list, [REDACTED] discovered that it had not revoked the access rights of the eight individuals. On that same date, [REDACTED] revoked the access rights.
- 217. The Alleged Violation affected [REDACTED]
[REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]
[REDACTED]
- 218. The Alleged Violation started on January 1, 2017, when [REDACTED] should have revoked the former contractors' physical access rights, and ended on June 6, 2017, when [REDACTED] revoked the access rights.

Description of Alleged Violation for [REDACTED]

- 219. On September 12, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation with CIP-004-6 R5; P5.1. See Self-Report, **Attachment 11b.** [REDACTED] did not timely revoke two individuals' unescorted physical access to

⁴⁵ The Alleged Violation was self-reported under R5.2; however, the Regions determined that R5.1 is the applicable Requirement.



BCSs within 24 hours from termination.

220. In the first instance, a co-op employee's employment ended on December 6, 2016, but [REDACTED] did not revoke the former employee's unescorted physical access to five PSPs until December 8, 2016. [REDACTED] discovered this instance in January 2017, during a monthly termination review.
221. In the second instance, an employee retired on June 1, 2017, but [REDACTED] did not revoke the former employee's unescorted physical access to five PSPs until June 21, 2017. [REDACTED] discovered this instance in July 2017, during a monthly termination review.
222. The Alleged Violation affected [REDACTED] and [REDACTED].
223. The duration of the first instance started on December 7, 2016, when [REDACTED] should have revoked the former employee's unescorted physical access rights, and ended on December 8, 2016, when [REDACTED] revoked the access rights. The duration of the second instance started on June 2, 2017, when [REDACTED] failed to revoke the former employee's unescorted physical access rights, and ended on June 21, 2017, when [REDACTED] revoked the access rights.

Description of Alleged Violation for [REDACTED]

224. On September 6, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-004-6 R5, P5.2.⁴⁶ See Self-Report, **Attachment 11c**. [REDACTED] did not timely revoke electronic access of an individual who no longer needed such access.
225. On May 24, 2016, [REDACTED] sent a notification to a [REDACTED] facilities contracting manager about a contractor whose training was set to expire on July 8, 2016. On June 23, 2016, the contractor's manager responded that the contractor no longer required physical access starting immediately. On June 28, 2016, the [REDACTED] directed the training director, the employee's supervisor, the regional facility asset manager, and the contractor's manager to commence revocation of access. On June 30, 2016, [REDACTED] reviewed an ad-hoc training completion report to verify that the contractor either attended training or [REDACTED] revoked access. The [REDACTED] discovered that the contractor still had access rights. On July 14, 2016, the [REDACTED] revoked the individual's access rights.

⁴⁶ The Alleged Violation was self-reported under CIP-004-6 R2.3; however, the Regions determined that CIP-004-6 R5.2 is the applicable Standard and Requirement.



employees and one contractor from a backup server by the end of the next calendar day following reassignment or transfer after receiving multiple requests to revoke access for these individuals between March 7 and May 13, 2017. One of the individuals involved had an elevated administrator role.

233. The Alleged Violation affected [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]
234. The Alleged Violation started on March 8, 2016, when [REDACTED] was first late in revoking electronic access rights from the secondary server, and ended on July 12, 2017, when [REDACTED] removed all seven individuals' electronic access rights from the secondary server.

Description of Alleged Violation for [REDACTED]

235. On December 4, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-004-6 R5; P5.2. *See* Self-Report, **Attachment 11f.** [REDACTED] did not timely revoke one individual's electronic access following reassignment where access was no longer needed.
236. On February 26, 2017, a manager determined that because of a reassignment in job duties an employee no longer required access to a CIP repository containing passwords to three medium impact BCAs. The manager entered access revocation information in the software system used to manage CIP access; however, the revocation of access did not occur because the owner of the CIP repository failed to perform additional steps required to complete the access revocation. [REDACTED] discovered this noncompliance on April 1, 2017, while performing a quarterly CIP access review, and revoked the individual's access on August 9, 2017.
237. The Alleged Violation affected [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]
238. The Alleged Violation started on February 28, 2017, when [REDACTED] was required to revoke the employee's electronic access to the CIP repository, and ended on August 9, 2017, when [REDACTED] revoked the employee's electronic access to the repository.



Aggregate Risk Assessment for CIP-004-6 R5 Alleged Violations

248. The Regions determined that the Alleged Violation posed an aggregate serious and substantial risk⁵⁰ to the reliability of the Bulk Power System (BPS) based on the following factors.⁵¹ The risk posed by these Alleged Violations was providing the opportunity for personnel who should no longer have access to BCSs, to access such systems. For all Alleged Violations, [REDACTED] had physical and electronic access logging and monitoring for incident detection and response. Additionally, [REDACTED] provided training and security awareness to assist employees' identification of suspicious and/or malicious behavior. Therefore, had an employee noticed suspicious activity, the employee should have known the proper actions. Regarding the third, fourth, fifth, sixth, and seventh (first instance) Alleged Violations, all individuals with unauthorized access or access to BCSs that were not needed were [REDACTED] employees, were properly granted access to BCSs, were current on cyber security training, and had a current PRA on file when access was granted thus reducing the likelihood that the individuals would use the unauthorized access in a way that would compromise the BPS.
249. Notwithstanding, the aggregate risk remains serious and substantial based on several factors. Between March 8, 2016 and September 29, 2017, [REDACTED] individuals maintained access to BCSs that were no longer needed. The Regions determined that [REDACTED] had serious, systemic security and compliance issues across its [REDACTED] functional groups, which required [REDACTED] to overhaul its entire CIP compliance program. Because of this, risk for continued noncompliance and compromise to BCSs and CAs dramatically increased. Due to the weaknesses in [REDACTED] CIP compliance program, the Regions anticipate that [REDACTED] will identify additional instances of noncompliance while completing mitigation, which [REDACTED] will report to the Regions. Notwithstanding, [REDACTED] comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that [REDACTED] reports.

Mitigation Actions for CIP-004-6 R5 Alleged Violations

250. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-004-6 R5 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.

⁵⁰ Alleged Violations [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] individually, posed a moderate risk to the reliability of the BPS, and [REDACTED] [REDACTED] individually, posed a minimal risk.

⁵¹ CIP-004-6 R5 has a VRF of "Medium" pursuant to the CIP-004-6 Table of Compliance Elements. According to the VSL Matrix, this violation warranted a "Moderate" VSL.



251. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED]: (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
252. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

K. CIP-005-1 (and 3a) R1 [REDACTED]
[REDACTED]

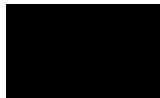
253. CIP-005-1 (and 3a) protects Cyber Assets by requiring the identification and protection of the Electronic Security Perimeter inside which all Critical Cyber Assets reside, as well as all access points on the Electronic Security Perimeter.
254. CIP-005-1 (and 3a) R1 provides:
- R1.** Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
 - R1.1.** Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
 - R1.2.** For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.



- R1.3.** Communication links connecting discrete Electronic Security Perimeter(s) shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
- R1.4.** Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.
- R1.5.** Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP003; Standard CIP-004 Requirement R3; Standard CIP-005 Requirements R2 and R3; Standard CIP-006 Requirement R3; Standard CIP-007 Requirements R1 and R3 through R9; Standard CIP-008; and Standard CIP-009.
- R1.6.** The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s), and the Cyber Assets deployed for the access control and monitoring of these access points.

Description of Alleged Violation for [REDACTED]

- 255. On February 26, 2016, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-005-1 R1.4. *See* Self-Report, **Attachment 12a.** [REDACTED] failed to identify and protect a non-critical Cyber Asset (non-CCA) within a defined Electronic Security Perimeter (ESP).
- 256. In April 2013, while conducting a cyber vulnerability assessment walk-down of its [REDACTED] [REDACTED] [REDACTED] discovered an undocumented [REDACTED] switch. The switch was associated with a simulation-training lab for the [REDACTED] which resided on a separate floor from the [REDACTED] [REDACTED] initially determined that the switch was out of scope with CIP-005 R1 because it was on a separate floor from the [REDACTED] and it was not an electronic access point to the ESP.
- 257. In November 2014, during a walk down of the [REDACTED] [REDACTED] reevaluated the device and again determined this device as not in scope of CIP because it was a simulation lab network device in a separate geographic location. Between June 2015 and September 2015, [REDACTED] began its transition to CIP version 5 and determined that the device was a CIP Protected Cyber Asset, and that the device was a non-CCA under CIP version 1 as far back as July 1, 2009.



258. The Alleged Violation started on January 2, 2010, when the Standard became mandatory and enforceable, and ended on September 30, 2015, when [REDACTED] placed the switch on the CCA list and afforded the switch the required CIP-005-3 protective measures.

Description of Alleged Violation for [REDACTED]

259. On April 7, 2015, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-005-3a R1.4. *See* Self-Report, **Attachment 12b**. [REDACTED] failed to identify and protect a non-CCA within a defined ESP.
260. On February 11, 2015, while performing a Cyber Asset (CA) evaluation before the CIP version 5 effective date, [REDACTED] discovered that a Human Machine Interface (HMI) was connected to the ESP but was not identified and afforded the protective requirements of CIP-005-3. HMI is a software application that provides a textual or graphical view of system conditions and operations to operators and allows the operators to implement control instructions for automated systems. On January 27, 2015, the technician removed the existing HMI, which was not connected to the ESP, and replaced it with the new HMI, but mistakenly connected it to the ESP.
261. The Alleged Violation started on January 27, 2015, when [REDACTED] connected the HMI to the ESP, and ended on February 13, 2015, when [REDACTED] disconnected the HMI from the ESP.

Description of Alleged Violation for [REDACTED]

262. On February 21, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-005-3a R1.4. *See* Self-Report, **Attachment 12c**. This Alleged Violation involves two instances where [REDACTED] failed to identify and protect a non-CCA within a defined ESP.
263. On October 7, 2015, between 3:15 p.m. and 3:55 p.m., and again on October 8, 2015, between 8:30 a.m. and 12:30 p.m., a security specialist at a [REDACTED] disconnected a network cable from the back of a CCA and plugged it into his laptop in an attempt to access email on the corporate network. [REDACTED] firewalls prevented the laptop from connecting to the corporate network.
264. The Information Technology (IT) security team discovered these instances of noncompliance during the investigation of abnormal multicast traffic in the network traffic logs and traced the activity back to the security specialist's laptop.
265. The first instance started on October 7, 2015, at 3:15 p.m., when the security specialist plugged the laptop into the ESP, and ended on October 7, 2015 at 3:45 p.m., when the security specialist removed the laptop from the ESP. The second

instance started on October 8, 2015, at 8:30 p.m., when the security specialist plugged the laptop into the ESP, and ended on October 8, 2015 at 12:30 p.m., when the security specialist removed the laptop from the ESP.

Description of Alleged Violation for [REDACTED]

266. On July 21, 2015, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as [REDACTED] [REDACTED] [REDACTED] and [REDACTED] they were in violation of CIP-005-3a R1.5 for failing to afford the protective measures specified in CIP-007-3a R5.1.3. *See* Self-Report, **Attachment 12d**.
267. CIP-007-3a R5.1.3, as applied to CIP-005-3a R1.5, required [REDACTED] to conduct annual reviews of user accounts to verify access privileges. In April 2015, [REDACTED] implemented a new Identity Access Management (IAM) tool, which assists in identifying CCAs and CCA user accounts. On April 1, 2015, during an internal discussion about the implementation of the new IAM tool, [REDACTED] discovered that Electronic Access Control and Monitoring (EACM) devices were not included in the 2014 CIP-007-3 R5 account verification review. [REDACTED] identified [REDACTED] EACM accounts that did not receive an annual review in 2014, nine of which had administrative privileges.
268. The Alleged Violation started on January 1, 2015, when the 2014 annual period expired and [REDACTED] had not performed an account verification review of the EACM devices, and ended on July 24, 2015, when [REDACTED] completed the EACM account verification review.

Description of Alleged Violation for [REDACTED]

269. On [REDACTED], [REDACTED] submitted a Self-Report, on behalf of [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-005-3a R1.5 for failing to afford the protective measures specified in CIP-005-3a R3 to one EACM Cyber Asset. *See* Self-Report, **Attachment 12e**.
270. CIP-005-3a R3, as applied to CIP-005-3a R1.5, requires [REDACTED] to implement an electronic or manual process for monitoring and logging access at access points to the ESP 24/7. On [REDACTED], while gathering evidence for an upcoming Compliance Audit, [REDACTED] discovered that one firewall, serving as an EACM CA, was not sending the security event logs to the centralized system logging and monitoring (syslog) server. The failure occurred on August 20, 2015, when a network card hardware failure occurred at the firewall, preventing the firewall from sending security event logs to the centralized server.
271. The Alleged Violation started on August 20, 2015, when electronic access monitoring and logging of the firewall ceased, and ended on October 21, 2015,

when electronic access logging and monitoring of the firewall resumed.

Description of Alleged Violation for [REDACTED]

272. On February 25, 2016, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-005-3a R1.5 for failing to afford the protective measures specified in CIP-007 R6. *See* Self-Report, **Attachment 12f**.
273. CIP-007 R6, as applied to CIP-005-3a R1.5, required [REDACTED] to ensure that all CAs within the ESP monitor system events related to cyber security. On April 21, 2015, [REDACTED] deployed new access control lists (ACLs) to several electronic access points on [REDACTED] EACM device routers. The routers were misconfigured, causing the electronic access points to block the centralized logging and monitor server logs associated with the [REDACTED] [REDACTED] switches from being sent to the security incident and event management (SIEM) device.
274. On April 22, 2015, a telecom compliance team analyst received an email from the SIEM stating that it had not received syslogs from the three associated switches. Upon further review, the analyst concluded that system logging was occurring on the local switches and dismissed the email alert from the SIEM as a false alarm. However, the analyst did not verify that the syslogs from the switches were actually transmitted from the syslog server to the SIEM. On October 7, 2015, during a quality assurance assessment on compliance documentation, [REDACTED] discovered that the three switches were not logging to the SIEM.
275. The Alleged Violation started on April 21, 2015, when electronic access logging and monitoring of the three switches ceased, and ended on October 7, 2015, when electronic access logging and monitoring of the switches resumed.

Aggregate Contributing Causes of CIP-005-1 (and 3a) R1 Alleged Violations

276. The primary cause of the CIP-005-1 (and 3a) R1 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] processes and internal controls did not require verification that syslogs of applicable CAs were being transmitted to EACM devices. Additionally, after upgrading the HMI, there was no secondary review or sign-off prior to connecting the HMI to the ESP. For all Alleged Violations, training could have helped prevent the Alleged Violations. For example, on at least two occasions, [REDACTED] assessed the misclassified [REDACTED] switch that was on a different floor than the [REDACTED] and on each occasion, incorrectly concluded that the switch should not be classified as a protected non-CCA. Additionally, the security guard who disconnected a cable

attached to a CCA and connected it to his laptop was unaware that he was connecting to the ESP. Moreover, the individual responsible for CIP protections of EACM devices was not aware that EACM devices were also protected under CIP-005-1 (and 3a) R1. Additional training, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violations.

Aggregate Risk Statement for CIP-005-1 (and 3a) R1 Alleged Violations

277. The Regions determined that the Alleged Violations posed an aggregate serious⁵² risk to the reliability of the Bulk Power System based on the following factors.⁵³ The risk posed by [REDACTED] failure to identify and protect non-CCAs within its ESP was the providing the opportunity for security incidents to go undetected, which could compromise [REDACTED] ability to quickly identify potential issues caused by such events. However, [REDACTED] did implement the following protective measures. Regarding the Alleged Violation where the security guard connected a laptop to the ESP, the ESP firewall blocked the computer from connecting to the corporate network. Additionally, regarding the Alleged Violation involving the unverified EACM user accounts, the accounts were assigned to authorized users, which were the same users (no changes) whose accounts were verified during the previous annual account verification. And, the Alleged Violation involving the HMI that was erroneously connected to the ESP, the HMI had no Internet connectivity, and the duration for that Alleged Violation was only 17 days.
278. Despite these protective measures, the aggregate risk remains serious and substantial based on several factors. From January 2, 2010 through August 8, 2015, [REDACTED] failed to identify and protect multiple CAs inside multiple ESPs. For instance, in the fourth Alleged Violation, [REDACTED] [REDACTED] were not included in [REDACTED] annual verification review. Additionally, in the fifth Alleged Violation, for over two months, a firewall, serving as an EACM and access point to an ESP, was not sending security event logs to the syslog server. In the sixth Alleged Violation, for over five months, electronic access points blocked the centralized logging and monitoring syslogs associated with [REDACTED] [REDACTED] switches from being sent to the SIEM device. In all three of these Alleged Violations, there was an increased risk that [REDACTED] would be unable to quickly identify potential issues caused by security events.

⁵² Alleged Violations [REDACTED], individually, posed a moderate risk to the reliability of the BPS, and [REDACTED], individually, posed a minimal risk.

⁵³ CIP-005-1 (and 3a) has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this noncompliance warranted a “Severe” VSL.



279. In addition, the Regions determined that [REDACTED] had serious, systemic security and compliance issues across its [REDACTED] functional groups, which required [REDACTED] to overhaul its entire CIP compliance program. Moreover, due to the weaknesses in [REDACTED] CIP compliance program, the Regions anticipate that [REDACTED] will identify additional instances of noncompliance while completing mitigation, which [REDACTED] will report to the Regions. Notwithstanding, [REDACTED] comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that [REDACTED] reports.

Mitigating Actions for CIP-005-1 (and 3a) R1 Alleged Violations

280. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-005-1 and 3a R1 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
281. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
282. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

L. CIP-005-5 R1 [REDACTED]
[REDACTED]

283. CIP-005-5 ensures the management of electronic access to 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.



284. CIP-005-5 R1 provides in relevant part:

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.

....

P1.3. Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

....

P1.5. Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

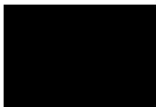
Description of Alleged Violation for [REDACTED]

285. During a Compliance Audit conducted [REDACTED], the Regions determined that [REDACTED] and [REDACTED] as [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED] were in violation of CIP-005-5 R1; P1.3. *See* PV Summary, **Attachment 13a.** [REDACTED] did not deploy deny access by default on two Electronic Security Perimeter (ESP) firewalls.

286. From a sample of ESP electronic access points, the audit team reviewed inbound and outbound access control permissions and discovered two instances where deny access by default was not deployed. In the first instance, an access control list (ACL) on an ESP firewall allowed interactive simple network management protocol (SNMP) communications from all hosts on non-ESP networks to Cyber Assets (CAs) within the ESP.

287. In the second instance, an ACL on an ESP firewall allowed SNMP and file transfer protocol (FTP) from all hosts on non-ESP networks to CAs within the ESP. In both instances, [REDACTED] failed to configure the ACLs to limit the hosts from the non-ESP networks to the CAs within the ESP. The ACLs permitted SNMP and FTP interactive access from all hosts on identified [REDACTED] virtual private networks to [REDACTED] [REDACTED] [REDACTED]

288. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on November 16, 2016, when [REDACTED] reconfigured the ACLs to limit access.

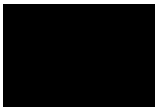


Description of Alleged Violation for [REDACTED]

289. On January 18, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-005-5 R1; P1.3. *See* Self-Report, **Attachment 13b**. [REDACTED] did not restrict inbound electronic access to [REDACTED] [REDACTED] ESPs.
290. On [REDACTED], while preparing for an upcoming Compliance Audit, the [REDACTED] firewall management team discovered that inbound and outbound access control permissions on [REDACTED] [REDACTED] firewalls were configured to allow connections to “any” host. Upon further review, [REDACTED] determined that on July 1, 2016, during its transition to CIP version 5, the firewall management team [REDACTED] [REDACTED] [REDACTED] [REDACTED], the software defaulted to “any” access permissions, which allowed [REDACTED] subnetworks outside the ESP to connect to any subnetwork host inside the ESP.
291. The Alleged Violation started on July 1, 2016, when [REDACTED] [REDACTED] [REDACTED] prompting the firewall software to default to “any” access permissions, and ended October 30, 2016, when [REDACTED] updated its firewall rules to restrict inbound access.

Description of Alleged Violation for [REDACTED]

292. On January 26, 2018, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-005-5 R1; P1.3. *See* Self-Report, **Attachment 13c**. [REDACTED] did not deny inbound and outbound access for unnecessary Internet Protocol (IP) addresses associated with ESP access points.
293. On December 5, 2016, [REDACTED] retired 10 BES Cyber Assets (BCAs) from service. On September 28, 2017, during a review of retired BCAs associated with a decommissioned BCS, [REDACTED] noticed that a number of the retired BCA IP addresses had not been removed from the associated firewall rulesets. [REDACTED] sampled additional firewall rulesets and discovered additional unnecessary IP addresses associated with [REDACTED] decommissioned BCAs.
294. The Alleged Violation started on December 5, 2016, when [REDACTED] retired the BCAs but did not remove the related IP addresses from the associated firewall rulesets, and ended on October 18, 2017, when [REDACTED] decommissioned the [REDACTED] [REDACTED] network environment associated with the firewalls in question.



Description of Alleged Violation for [REDACTED]

- 295. On April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-005-5 R1; P1.5. *See* Self-Report, **Attachment 13d**. [REDACTED] did not monitor for malicious communications for an ESP.
- 296. On January 11, 2017, [REDACTED] completed a service request to replace data network switches inside a [REDACTED] ESP. On February 28, 2017, during a review of the newly implemented changes to the ESP, [REDACTED] discovered that its intrusion detection system (IDS) test access points (TAPs) were not monitoring ESP inbound and outbound communications. [REDACTED] conducted an investigation and found that it failed to properly connect the IDS TAPs cables to the new data network switches.
- 297. The Alleged Violation started on January 11, 2017, when [REDACTED] improperly connected the IDS TAPs cables to the data network switches preventing monitoring for malicious communications, and ended on March 2, 2017, when [REDACTED] properly connected the IDS TAPs cables to the new data network switches and confirmed monitoring for malicious ESP communications was fully implemented.

Aggregate Contributing Causes of CIP-005-5 R1 Alleged Violations

- 298. The primary cause of the CIP-005-1 R1 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. For three of the four Alleged Violations, [REDACTED] processes did not clearly define the roles and responsibilities and specific steps needed to ensure compliance. Specifically, regarding CIP-005-5 R1; P1.3, [REDACTED] process for configuring access control permissions lacked specific steps to ensure the firewalls were configured correctly, which resulted in inconsistent application of the process. Additionally, the process did not clearly identify data network connections that include TAPs, and the roles and responsibilities were not clearly defined as to who was responsible to monitor the IDS and respond to security events reported by IDS. Regarding CIP-005-5 R1; P1.5, after decommissioning BCSs, there were no secondary reviews to ensure that unnecessary BCA IP addresses had been removed from the associated firewall rulesets. Additional training, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violations.

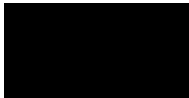


Mitigating Actions for CIP-005-5 R1 Alleged Violations

301. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-005-5 R1 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
302. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED]: (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
303. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

M. CIP-005-3a R2 [REDACTED]

304. CIP-005-3a protects Cyber Assets by requiring the identification and protection of the ESP inside which all Critical Cyber Assets reside, as well as all access points on the Electronic Security Perimeter.
305. CIP-005-3a R2 provides:
 - R2.** Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
 - R2.1.** These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.



- R2.2.** At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
- R2.3.** The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
- R2.4.** Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
- R2.5.** The required documentation shall, at least, identify and describe:
 - R2.5.1.** The processes for access request and authorization.
 - R2.5.2.** The authorization methods.
 - R2.5.3.** The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement 4.
 - R2.5.4.** The controls used to secure dial-up accessible connections.

Description of Alleged Violation for [REDACTED]

- 306. On July 25, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as [REDACTED] they were in violation of CIP-005-3a R2.1, R2.2, and R2.4.⁵⁶ See Self-Report, **Attachment 14a**. [REDACTED] did not implement organizational processes and technical and procedural mechanisms for controlling electronic access at all electronic access points to its Electronic Security Perimeter (ESP).
- 307. [REDACTED] used overly broad Internet Protocol (IP) address space in ESP firewall rulesets such that explicit deny by default was not implemented per R2.1. On June 20, 2017, during a cyber vulnerability assessment of a [REDACTED] ESP, [REDACTED] discovered it had granted [REDACTED] individuals of the [REDACTED] [REDACTED] unauthorized access to the ESP via an unprotected [REDACTED] [REDACTED] located inside the associated Physical Security Perimeter (PSP).
- 308. Upon further review, [REDACTED] discovered it had also provided the [REDACTED] unauthorized access, via the [REDACTED], to a [REDACTED] ESP. The firewall electronic access points to the ESPs and the [REDACTED] were located in the same physical modular network switches. Because of the overly

⁵⁶ The Alleged Violation was self-reported under CIP-005-5 R1; P1.3; however, the Regions determined that CIP-005-3a R2.1, R2.2, and R2.4 are the applicable Standard Requirements because of the start date of the Alleged Violation.

██████████

broad ESP firewall rulesets, ESP traffic was not blocked on the data network physical interface ██████████ connecting the unprotected ██████████, which was used to manage the hosts in the ██████████.

309. Because ██████████ used overly broad ESP firewall rulesets, access was permitted across ports and services that were not required for operations or for monitoring Cyber Assets (CAs) within the ESPs (R2.2). Additionally, ██████████ failed to implement strong technical controls to ensure the authenticity of the accessing party for the ██████████ individuals who were granted unauthorized access to the ESPs (R2.4).
310. The Alleged Violation started on January 11, 2017, the day following the previous CIP Compliance Audit, through June 27, 2017, when ██████████ reconfigured the firewall rulesets preventing unauthorized access into the ESPs.

Description of Alleged Violation for ██████████

311. On June 22, 2017, ██████████ submitted a Self-Report to ██████████ on behalf of ██████████ stating that, as a ██████████ ██████████ was in violation of CIP-005-3a R2.2. *See* Self-Report, **Attachment 14b**. ██████████ failed to disable one port that was not required for the operations or monitoring CAs within the ESP.
312. On April 13, 2017, during preparation to move legacy printer queues from ██████████-related print servers, ██████████ discovered that the firewall ruleset previously used to connect the printer inside the ██████████ ESP to a corporate print server was no longer required. Upon further review, ██████████ discovered that on January 18, 2016, the old printer was replaced with a different model. The port used for the old printer was no longer required, but ██████████ failed to disable the port.
313. The Alleged Violation started on January 18, 2016, when the printer port was no longer needed, and ended on April 28, 2017, when ██████████ disabled the unnecessary port.

Description of Alleged Violation for ██████████

314. On August 28, 2015, ██████████ submitted a Self-Report to ██████████ on behalf of ██████████ stating that, as a ██████████ and ██████████ it was in violation of CIP-005-3a R2.5.3.⁵⁷ *See* Self-Report, **Attachment 14c**. ██████████ failed to timely update its Critical Cyber Asset (CCA) access list in accordance with CIP-004-3 R4.
315. CIP-004-3 R4, as applied to CIP-005-3a R2.5.3, required ██████████ to maintain lists of personnel with authorized cyber or unescorted physical access to CCAs. On May 20, 2015, during a quarterly review of ██████████ CCA access list, ██████████ discovered

⁵⁷ The Alleged Violation was self-reported under CIP-005-3a R1.5; however, the Regions determined that CIP-005-1 R2.5.3 is the applicable Standard and Requirement.

[REDACTED]

that it failed to update its CCA access list for personnel with authorized cyber or unescorted physical access to its Electronic Access Control and Monitoring (EACM) servers within seven days of a change in access rights. Specifically, [REDACTED] removed one unique user account to [REDACTED] EACM servers, provisioned access for a user account to [REDACTED], provisioned a shared user account on [REDACTED] EACM servers for resetting passwords and support changes, and provisioned a shared user account on [REDACTED] that provided access for [REDACTED] support administrators. However, [REDACTED] did not update the CCA access list to reflect these changes in access rights.

316. The Alleged Violation started on January 23, 2013, the earliest date [REDACTED] provisioned access to an account but did not update the CCA access list, and ended on July 28, 2015, when [REDACTED] updated the CCA access list to include all changes of access rights.

Aggregate Contributing Causes of CIP-005-3a R2 Alleged Violations

317. The primary cause of the CIP-005-3a R2 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient electronic access control process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] processes did not clearly define the roles and responsibilities and specific steps needed to ensure compliance. [REDACTED] did not have a formal process to validate separation of BES and non-BES networks, and there was no secondary review of changes to the configuration of electronic access points. Additionally, the process did not clearly define the roles and responsibilities for firewall changes and updating CCA access lists, which resulted in inconsistent application of the process. Further, there was no secondary review of firewall changes to ensure that existing ports were assessed for applicability. Additional training, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violations.

Aggregate Risk Statement for CIP-005-3a R2 Alleged Violations

318. The Regions determined that the Alleged Violations posed an aggregate serious and substantial risk⁵⁸ to the reliability of Bulk Power System.⁵⁹ The risk posed by [REDACTED] failure to properly control electronic access at all electronic access points to its ESPs was providing the opportunity for unauthorized access to CAs and CCAs

⁵⁸ Alleged Violation [REDACTED], individually, posed a serious risk to the reliability of the BPS, [REDACTED] individually, posed a moderate risk, and [REDACTED], individually, posed a minimal risk.

⁵⁹ CIP-005-3a R2.1, R2.2, R2.4 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “High” VSL.

inside the ESPs. However, [REDACTED] did implement the following protective measures. Regarding the first Alleged Violation, although [REDACTED] failed to block the ESP traffic between the ESP and unprotected [REDACTED], the [REDACTED], which was used to manage the [REDACTED], was configured to only allow access to non-ESP data. Thus, no ESP data could be transmitted to the [REDACTED], and the [REDACTED] were unable to transmit data to protected systems residing within the ESP. Regarding the third Alleged Violation where [REDACTED] failed to update the CCA access list to reflect changes in access rights to EACM servers, all individuals who gained access to the new EACM server accounts were authorized to have access to the accounts, were up-to-date on cyber security training, and had current PRAs on file.

319. Despite these protective measures, the aggregate risk remains serious and substantial because, in the first Alleged Violation, there were [REDACTED] affected user accounts, multiple unnecessary open ports and services, [REDACTED] failed to ensure the authenticity of the accessing party of the unauthorized users, and the duration of the Alleged Violation was over five years.

Mitigating Actions for CIP-005-3a R2 Alleged Violations

320. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-005-3a R2 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
321. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED]: (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
322. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED].

completion of the Mitigation Activities and promptly report its successful completion to NERC.

M. CIP-005-5 R2

323. CIP-005-5 requires the management of electronic access to BES Cyber Systems by specifying a controlled ESP in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
324. CIP-005-5 R2 provides:
- 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.
 - P2.1.** Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
 - P2.2.** For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.
 - P2.3.** Require multi-factor authentication for all Interactive Remote Access sessions.

Description of Alleged Violation for

325. On [REDACTED], [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-005-5 R2; P2.1. *See* Self-Report, **Attachment 15a**. Also on [REDACTED], [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as [REDACTED] and [REDACTED] they were in violation of CIP-005-5 R2; P2.1. *See* Self-Report, **Attachment 15b**.⁶⁰ This Alleged Violation involved two instances where [REDACTED] allowed interactive remote access to BES Cyber Systems (BCSs) inside [REDACTED] Electronic Security Perimeter (ESP) without first going through an Intermediate System.
326. In the first instance, on July 1, 2015, [REDACTED] commissioned a [REDACTED] with Critical Cyber Assets (CCAs) and implemented technical controls at the electronic access points to ensure authenticity of the accessing party for interactive remote access in accordance with CIP-005-3a R2.4. CIP-005-5 became effective on [REDACTED] [REDACTED] and requires an Intermediate System to restrict direct interactive remote

⁶⁰ This self-reported noncompliance was assigned NERC Tracking Number [REDACTED], but was administratively dismissed and consolidated with [REDACTED] on January 25, 2017.

[REDACTED]

access to medium and high impact BCSs. On [REDACTED], in preparation for a CIP version 5 Compliance Audit, [REDACTED] conducted a review of its [REDACTED] firewall and core router access control rules and discovered that it permitted interactive remote access between each of the [REDACTED] [REDACTED] and the [REDACTED] [REDACTED] without first going through an Intermediate System. As a result, [REDACTED] staff could directly access the [REDACTED] from Cyber Assets (CAs) residing outside the ESP.

327. In the second instance, in May 2015, while transitioning to CIP version 5, [REDACTED] performed its initial identification assessment of Intermediate Systems that support interactive remote access. On [REDACTED], in preparation for an upcoming CIP Compliance Audit, the [REDACTED] Quality Assurance team discovered [REDACTED] servers that [REDACTED] did not identify as Intermediate Systems in its initial assessment. The servers are the platform that hosts the virtual hosts where the interactive remote access connects. [REDACTED] deployed [REDACTED] of the [REDACTED] servers inside the ESP; however, the servers are required to be outside the ESP to restrict remote access directly to BCSs inside the ESP.
328. In addition, [REDACTED] did not properly identify the remaining [REDACTED] servers as Electronic Access Control and Monitoring System (EACMS) devices during its initial identification of intermediate devices in May of 2015. As a result, [REDACTED] failed to provide the protective measures specified in CIP-007-6 P1.1⁶¹, P.2.3⁶², P2.4⁶³, P4.2⁶⁴, P5.2⁶⁵, P5.7⁶⁶, and CIP-010-2 R1; P1.1 – P1.5⁶⁷, R2; P2.1⁶⁸, and R3; P3.1 – P3.4.⁶⁹
329. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED] when [REDACTED] committed

⁶¹ CIP-007-6 P1.1 requires [REDACTED] to ensure that only logical network accessible ports that are needed are enabled for these EACM devices.

⁶² CIP-007-6 P2.3 requires [REDACTED] to create a mitigation plan to mitigate the vulnerabilities addressed by each applicable security patch and timeframe to complete these mitigations.

⁶³ CIP-007-6 P2.4 requires [REDACTED] to create to implement the mitigation plan for these EACMS devices within the timeframe specified in the plan.

⁶⁴ CIP-007-6 P4.2 requires the EACMS devices to generate alerts for security events.

⁶⁵ CIP-007-6 P5.2 requires [REDACTED] to identify and inventory all known enabled default or other generic account types, which includes EACMS devices.

⁶⁶ CIP-007-6 P5.7 requires [REDACTED] to either limit the number of unsuccessful attempts or generate alerts after a threshold of unsuccessful authentication attempts for the EACMS devices.

⁶⁷ CIP-010-2 R1; P1.1 – P1.5 requires [REDACTED] to implement its Configuration Change Management Program (baseline configurations) on these EACMS devices.

⁶⁸ CIP-010-2 R2; P2.1 requires [REDACTED] to implement configuration monitoring on these EACMS devices.

⁶⁹ CIP-010-2 R3; P3.1 – P3.4 requires [REDACTED] to conduct and document vulnerability assessments on these EACMS devices.

to complete its Mitigation Plan.

Description of Alleged Violation for [REDACTED]

330. On [REDACTED], [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-005-5 R2; P2.1.⁷⁰ See Self-Report, **Attachment 15c.** [REDACTED] allowed interactive remote access to BCSs inside [REDACTED] ESPs without first going through an Intermediate System.
331. On [REDACTED], while collecting evidence for an upcoming Compliance Audit, [REDACTED] discovered that firewall rulesets were configured to allow external interactive remote access to [REDACTED] ESP networks at [REDACTED] facilities without first going through an Intermediate System.
332. The Alleged Violation began on July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED], when [REDACTED] committed to complete its Mitigation Plan.

Description of Alleged Violation for [REDACTED]

333. On June 22, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] was in violation of CIP-005-5 R2; P2.1. See Self-Report, **Attachment 15d.** [REDACTED] allowed interactive remote access to BCSs inside [REDACTED] ESPs without first going through an Intermediate System.
334. On May 23, 2016, [REDACTED] commissioned two control centers. During this process, firewall rulesets were configured to allow [REDACTED] workstations interactive remote access to BCSs inside the [REDACTED] ESPs without first going through an Intermediate System. As a result, the [REDACTED] workstations initiating interactive remote access had direct access to BCSs inside the ESP. On March 29, 2017, during annual firewall reviews, [REDACTED] discovered the issue and changed the firewall rulesets to remove the unauthorized remote access from the [REDACTED] workstations.
335. The Alleged Violation began on July 1, 2016, when the Standard became mandatory and enforceable, and ended on March 29, 2017, when [REDACTED] changed the firewall rulesets to preclude the [REDACTED] workstations from directly accessing BCSs inside the ESPs.

⁷⁰ The Alleged Violation was self-reported under CIP-005-5 R1; P.1.3; however, the Regions determined that CIP-005-5 R2; P2.1 is the applicable Standard and Requirement.



Description of Alleged Violation for [REDACTED]

336. During a Compliance Audit conducted [REDACTED], the Regions determined that [REDACTED] and [REDACTED] as [REDACTED] [REDACTED] [REDACTED] and [REDACTED] were in violation of CIP-005-5 R2; P2.1, P2.2, and P2.3. See PV Summary, **Attachment 15e**. From a sample of ESP inbound and outbound access control permissions, the audit team discovered that [REDACTED] allowed interactive remote access to BCSs inside [REDACTED] ESP without first going through an Intermediate System, utilizing encryption, and requiring multi-factor authentication.
337. The audit team discovered [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
338. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED] when [REDACTED] committed to complete its Mitigation Plan.

Description of Alleged Violation for [REDACTED]

339. On August 8, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] was in violation of CIP-005-5 R2; P2.1, P2.2, and P2.3. See Self-Report, **Attachment 15f**. [REDACTED] allowed interactive remote access to BCSs inside [REDACTED] ESPs without first going through an Intermediate System, utilizing encryption, and requiring multi-factor authentication.
340. On June 26, 2017, [REDACTED] discovered that on June 23, 2017, during application testing and validation associated with an [REDACTED] upgrade project, [REDACTED] BCAs were used by [REDACTED] personnel to initiate interactive remote access to [REDACTED] [REDACTED] servers inside the ESPs at a [REDACTED] and [REDACTED] without first going through an Intermediate System. [REDACTED] determined that on February 17, 2016, it incorrectly configured the firewalls to grant access to a wide range of ports, including the port

⁷¹ CIP-005-5 R2 has a VRF of “Medium” pursuant to the CIP-005-5 Table of Compliance Elements. According to the VSL Matrix, this violation warranted a “High” VSL.



range used for interactive remote access.

- 341. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on June 28, 2017, when [REDACTED] disabled the port range firewall rule that was used for interactive remote access.

Aggregate Contributing Causes of CIP-005-5 R2 Alleged Violations

- 342. The primary cause of the CIP-005-5 R2 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient interactive remote access management process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] processes did not clearly define the roles and responsibilities and specific steps needed to ensure compliance. Specifically, the process did not provide clarity on identifying interactive remote access communications when reviewing firewall rules. Additionally, the process did not include prohibiting interactive remote access where systems-to-systems communications were permitted. [REDACTED] staff was not adequately trained on the differences between version 3 and version 5, which created process deficiencies and confusion on the implementation of [REDACTED] version 5 program. Additional training, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violations.

Aggregate Risk Statement for CIP-005-5 R2 Alleged Violations

- 343. The Regions determined that the Alleged Violations posed an aggregate serious and substantial risk⁷² to the reliability of the Bulk Power System based on the following factors.⁷³ [REDACTED] failures to identify and correctly deploy Intermediate Systems to restrict interactive remote access allows direct access to BCSs. Without the Intermediate System, a remote computer could pass vulnerabilities directly to the BCS and affect BPS stability through unreliable operations and/or unavailability of the BCS. However, [REDACTED] did implement the following protective measures.

[REDACTED]

⁷² Alleged Violations [REDACTED], individually, posed a moderate risk to the reliability of the BPS, and [REDACTED] individually, posed a minimal risk.

⁷³ CIP-005-5 R2 has a VRF of “Medium” pursuant to the CIP-005-5 Table of Compliance Elements. According to the VSL Matrix, this violation warranted a “High” VSL.



344. Despite these protective measures, the aggregate risk remains serious and substantial based on several factors. For all Alleged Violations, CIP-005-5 R2 2.1 was not applied to any of the affected BCSs or CAs since the Standard became mandatory and enforceable on July 1, 2016. The Regions determined that [REDACTED] had serious, systemic security and compliance issues across its [REDACTED] functional groups, which required [REDACTED] to overhaul its entire CIP compliance program. Because of this, the risk for continued noncompliance and compromise to CIP BES Cyber Systems and Cyber Assets dramatically increased. Due to the weaknesses in [REDACTED] CIP compliance program, the Regions anticipate that [REDACTED] will identify additional instances of noncompliance while completing mitigation, which [REDACTED] will report to the Regions. Notwithstanding, [REDACTED] comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that [REDACTED] reports.

Mitigating Actions for CIP-005-5 R2 Alleged Violations

345. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-005-5.R2 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
346. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
347. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED]

completion of the Mitigation Activities and promptly report its successful completion to NERC.

N. CIP-006-3c R1 [REDACTED]

348. CIP-006 ensures that a Responsible Entity implements a physical security program for the protection of Critical Cyber Assets.

349. CIP-006-3c R1 provides in relevant part:

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

Description of Alleged Violation for [REDACTED]

350. On June 13, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-006-3c R1.1. *See Self Report, Attachment 16a.* [REDACTED] failed to maintain a completely enclosed six-wall Physical Security Perimeter (PSP) border after the completion of a facility upgrade.

351. On March 4, 2016, [REDACTED] completed a renovation project at an existing PSP at a [REDACTED]. On March 18, 2016, during a quality assurance site inspection performed by management, [REDACTED] discovered that the construction contractor left vents unsecured on the PSP border. Later that day, [REDACTED] secured the

opening by using [REDACTED]

352. The Alleged Violation started on March 4, 2016, when the [REDACTED] contractor completed the work without securing the vent openings, and ended on March 18, 2016, when [REDACTED] secured the vent openings.

Description of Alleged Violation for [REDACTED]

353. On July 21, 2015⁷⁴ and October 28, 2015, [REDACTED] submitted two Self-Reports to [REDACTED] on behalf of [REDACTED] and [REDACTED] stating that, as a [REDACTED] [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-006-3c R1.5. *See* Self-Reports, **Attachments 16b and 16c.**⁷⁵ Also on March 11, 2016, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as [REDACTED] and [REDACTED] they were in violation of CIP-006-3c R1.5. *See* Self-Report, **Attachment 16d.**⁷⁶ The Self-Reports include a total of four instances where [REDACTED] failed to properly provision physical access authorization requests in accordance with CIP-004-3 R4.1.
354. CIP-004-3 R4.1, as applied to CIP-006-3c, requires [REDACTED] to review the lists of its personnel who have access to Critical Cyber Assets (CCAs) quarterly, and update the lists within seven calendar days of any change of personnel with such access to CCAs, or any change in the access rights of such personnel.
355. In the first instance, on April 13, 2015, a work order was submitted to provide a [REDACTED] employee physical access rights to the PSPs in a [REDACTED], a [REDACTED], a [REDACTED] and a server room that is not located within a defined PSP. On April 16, 2015, at 3:07 p.m., an access services employee properly approved and granted the employee's access to the [REDACTED] PSP; however, the employee mistakenly approved and granted access to a trading floor PSP instead of the non-PSP server room, both of which are located in the same facility. At 3:26 p.m., during a review of completed work orders, the access services team discovered and revoked the unauthorized access. [REDACTED] verified that the individual did not utilize the unauthorized access.
356. In the second instance, on July 17, 2015, a [REDACTED] contractor requested approval for physical access to a [REDACTED] and [REDACTED] PSPs. The Manager responsible for approving the access request approved access to the [REDACTED]

⁷⁴ This noncompliance involves [REDACTED] for its [REDACTED] [REDACTED] and [REDACTED] functions.

⁷⁵ This self-reported noncompliance was assigned NERC Tracking Number [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on March 31, 2016.

⁷⁶ This self-reported noncompliance was assigned NERC Tracking Number [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on March 31, 2016. This noncompliance involves [REDACTED] for its [REDACTED] [REDACTED] [REDACTED] and [REDACTED] functions.



PSP but denied access to the [REDACTED] PSP. However, on July 21, 2015, the access services team erroneously approved the work order and granted access to both PSPs. On July 24, 2015, during a review of the internal control reports for granted access, the access services team discovered and revoked the unauthorized access.

357. In the third instance, on August 21, 2015, a [REDACTED] employee who was working on a temporary assignment requested physical access to [REDACTED] PSPs located within a control center and a [REDACTED]. On August 21, 2015, at 12:07 p.m., an access services employee erroneously approved and granted the requested access prior to the approval of the employee's manager. At 12:49 p.m., during a review of the internal control reports for granted access, the access services team discovered and revoked the unauthorized access.
358. In the fourth instance, on September 28, 2015, at 11:24 a.m., a work order was submitted to revoke an employee's physical access to [REDACTED] non-PSPs and to add access permission for one PSP. Due to system design limitations, the badge access system could not process NERC and non-NERC access requests or revocations on the same work order, so [REDACTED] access services team rejected the change request. However, the system failed to perform as expected and processed the request ticket as approved. The system processed the removal access requests at 11:25 a.m. [REDACTED] staff manually rejected the request to add access permissions to the CIP PSP because policy stated that add access requests and remove access requests could not be within the same work order.
359. At 1:42 p.m., the access services team discovered that even though the add request was manually rejected, the badging system had provisioned access to the employee's badge, and the access request was pending approval. At 11:07 p.m., the access control team logged into the badging system and observed the request was still awaiting approval. The access team manually rejected the add access request for the second time. However, prior to the second rejection, the system had auto-generated approval and granted the access permissions.
360. On September 29, 2015, the access services team received an email alert identifying the anomaly. However, the access services team failed to review the email until October 13, 2015. Upon review, [REDACTED] discovered that even though it manually rejected the employee access request to add access permissions, the system approved the employee for access and authorized the badge for access to the NERC CIP identified PSP. [REDACTED] discovered through an internal investigation that a badging system coding error permitted the approval of access even though the business rules specifically did not permit the system approval. In total, [REDACTED] found six individuals receiving PSP access authorizations under similar circumstances.



The managers approved the access, but the system granted access three days prior to the required manager approval.

361. The Alleged Violation started on April 16, 2015, at 3:07 p.m., when, in the first instance, [REDACTED] granted the employee unauthorized access rights to the PSP, and ended on October 13, 2015, when, in the fourth instance, the [REDACTED] manager approved the access request.

Description of Alleged Violation for [REDACTED]

362. On [REDACTED], [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-006-3c R1.6.2. *See* Self-Report, **Attachment 16e**. Also, on [REDACTED], [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-006-3c R1.6.1. *See* Self-Report, **Attachment 16f**.⁷⁷ During a Compliance Audit of [REDACTED] conducted [REDACTED], the Regions discovered an additional instance of noncompliance with CIP-006 R1.6. *See* PV Summary, **Attachment 16g**.⁷⁸ Between February 23, 2016 and June 30, 2016, [REDACTED] submitted four additional Self-Reports to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] [REDACTED] [REDACTED] and [REDACTED] they were in violation with CIP-006-3c R1.6. *See* Self-Reports, **Attachments 16h**,⁷⁹ **16i**,⁸⁰ **16j**,⁸¹ and **16k**.⁸² Following the Self-Reports, [REDACTED] conducted additional

⁷⁷ This self-reported noncompliance was assigned NERC Tracking Number [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on March 31, 2016. [REDACTED] was administratively dismissed and consolidated with [REDACTED] on June 13, 2016. This noncompliance involves [REDACTED] for its [REDACTED] and [REDACTED] functions.

⁷⁸ This noncompliance discovered during a Compliance Audit was assigned NERC Tracking Number [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on March 31, 2016. [REDACTED] was administratively dismissed and consolidated with [REDACTED] on June 13, 2016.

⁷⁹ This February 23, 2016 self-reported noncompliance was assigned NERC Tracking Number [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on March 31, 2016. [REDACTED] was administratively dismissed and consolidated with [REDACTED] on June 13, 2016. This noncompliance involves [REDACTED] for its [REDACTED] and [REDACTED] functions.

⁸⁰ This April 7, 2016 self-reported noncompliance was assigned NERC Tracking Number [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on March 31, 2016. [REDACTED] was administratively dismissed and consolidated with [REDACTED] on June 13, 2016. This noncompliance involves [REDACTED] [REDACTED] [REDACTED] and [REDACTED] for their [REDACTED] [REDACTED] and [REDACTED] functions.

⁸¹ This April 12, 2016 self-reported noncompliance was assigned NERC Tracking Number [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on March 31, 2016. [REDACTED] was administratively dismissed and consolidated with [REDACTED] on June 13, 2016. This noncompliance involves [REDACTED] for its [REDACTED] function.

⁸² This June 30, 2016 self-reported noncompliance was assigned [REDACTED] Tracking Number [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on July 12, 2016. This noncompliance involves [REDACTED] for its [REDACTED] function.

expansions of scope and identified many additional instances of noncompliance with CIP-006-3c R1.6.

363. [REDACTED] failed to document all the required information in its logbooks for visitors who accessed [REDACTED] PSPs as required by R1.6.1. Specifically, there were over 100 instances involving all of [REDACTED] PSPs with at least one missing log entry, including the escort name, escort badge number, and visitor PSP entry and exit times. Additionally, there were eight occasions where [REDACTED] failed to continuously escort visitors within multiple PSPs as required by R1.6.2.
364. The Alleged Violation started on February 23, 2015, the earliest date [REDACTED] failed to complete the logbook entries, and will end on [REDACTED] the date [REDACTED] committed to completing its Mitigation Plan.

Description of Alleged Violation for [REDACTED]

365. On August 11, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-006-3c R1.6.2. *See* Self-Report, **Attachment 16l**. [REDACTED] failed to continuously escort one visitor while inside a PSP.
366. On June 1, 2016, at 5:55 p.m., [REDACTED] experienced a Physical Access Control System outage that affected the central server but did not affect the local controller logging or access functions. In response to this outage, a [REDACTED] [REDACTED] posted a security guard at the PSP entry point to supervise manual logging. Relying on an outdated outage security plan, the security guard's supervisor gave the guard an emergency badge in case he needed to access the PSP.
367. At 6:28 p.m., a [REDACTED] employee, believing that the security guard was authorized to enter the [REDACTED] PSP because he possessed the emergency badge, allowed the security guard into the PSP to escort a cleaning contractor. The [REDACTED] employee logged his name in the logbook as the escort for the security guard and contractor and delegated the security guard as the escort for the contractor while inside the PSP.
368. The contractor had authorized unescorted access to the PSP and did not need an escort; however, the security guard did not have such access. Therefore, the [REDACTED] employee allowed the security guard to be inside the PSP without a continuous escort and inappropriately delegated the security guard as the escort for the contractor. The security guard's supervisor observed the security guard on closed circuit television and instructed the security guard to exit the PSP. The security guard left the PSP with the contractor at 8:55 p.m.

369. The Alleged Violation started on June 1, 2016, at 6:28 p.m., when the [REDACTED] employee left the security guard in the PSP unescorted, and ended on June 1, 2016, at 8:55 p.m., when the security guard exited the PSP.

Aggregate Root Causes of CIP-006-3c R1 Alleged Violations

370. The primary cause of the CIP-006-3c R1 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient electronic access control process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. Regarding the first Alleged Violation where [REDACTED] failed to complete a completely enclosed six-wall PSP border, [REDACTED] lacked an internal control to verify that the contractor completed all the required project tasks. Regarding the second Alleged Violation where [REDACTED] failed to properly provision physical access authorization requests, [REDACTED] access approval process did not clearly define the roles and responsibilities to ensure compliance. For instance, managers were required to follow different steps depending upon whether the worker was an employee or a contractor, and if a contractor, the steps were different for those sourced from a particular contingent workforce staffing agency and those sourced elsewhere. Such variations created confusion amongst the managers. Additionally, the process required two approvals, one automated and the other manual, which increased the risk for errors. Regarding the third Alleged Violation, there were no internal controls to limit over 100 instances of missing visitor log information within a 14-month period across [REDACTED] [REDACTED] functional groups. Regarding the fourth Alleged Violation, [REDACTED] failed to train the security guard and [REDACTED] employee who let the security guard inside the PSP on recent procedural changes. The new procedure no longer has provisions for an “Emergency Badge,” which caused confusion for the [REDACTED] employee. The [REDACTED] employee believed that the “Emergency Badge” authorized the security guard access within the PSP. Additional training, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violations.



Aggregate Risk Statement for CIP-006-3c R1 Alleged Violations

371. The Regions determined that the Alleged Violations posed an aggregate serious or substantial risk⁸³ to the reliability of the BPS.⁸⁴ The risk posed by the CIP-006-3c R1 Alleged Violations was providing the opportunity for unauthorized physical access to CCAs within the PSPs. Several factors increased the aggregate risk. In the third Alleged Violation, between February 2015 and April 2016, there were over one hundred instances of noncompliance involving all of [REDACTED] PSPs. The Regions determined that [REDACTED] had serious, systemic security and compliance issues across its [REDACTED] functional groups, which required [REDACTED] to overhaul its entire CIP compliance program. Because of this, risk for continued noncompliance and compromise to BCSs and CAs dramatically increased. Due to the weaknesses in [REDACTED] CIP compliance program, the Regions anticipate that [REDACTED] will identify additional instances of noncompliance while completing mitigation, which [REDACTED] will report to the Regions. Notwithstanding, [REDACTED] comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that [REDACTED] reports.

Mitigating Actions for CIP-006-3c R1 Alleged Violations

372. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-006-3c R1 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
373. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed

⁸³ Alleged Violation [REDACTED], individually, posed a serious risk to the reliability of the BPS, and [REDACTED] individually, posed a minimal risk.

⁸⁴ CIP-006-3c R1.6 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

374. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

O. CIP-006-6 R1 [REDACTED]
[REDACTED]

375. CIP-006-6 requires the management of physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
376. CIP-006-6 R1 provides in relevant part:
- 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.
 - P1.1.** Define operational or procedural controls to restrict physical access.
 - P1.2.** 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.
 - P1.4.** Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
 - P1.8.** 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.

Description of Alleged Violation for [REDACTED]

377. On February 9, 2018, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-006-6 R1; P1.1. *See* Self-Report, **Attachment 17a**. [REDACTED] did not implement physical access controls to allow only those personnel with authorized unescorted access to access one Physical Security Perimeter (PSP).
378. On November 29, 2017, at 4:31 p.m., an employee exited a PSP; however, before the PSP door fully closed, a package delivery person without authorized PSP access

[REDACTED]

swung open the door and entered the PSP. A [REDACTED] security officer posted near the PSP witnessed the unauthorized access, escorted the person outside the PSP, and reported the incident to management.

379. The Alleged Violation started on November 29, 2017, at 4:31 p.m., when the package delivery person entered the PSP, and ended on November 29, 2017, at 4:33 p.m., when the [REDACTED] security guard escorted the package delivery person outside the PSP.

Description of Alleged Violation for [REDACTED]

380. On September 8, 2016, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-006-6 R1; P1.2. *See* Self-Report, **Attachment 17b**. [REDACTED] did not implement physical access controls to allow only those personnel with authorized unescorted access to access three [REDACTED] PSPs.
381. On August 10, 2016, [REDACTED] [REDACTED] conducted an internal access category review in preparation for commissioning future NERC CIP sites and discovered that [REDACTED] had inappropriately assigned an access category to one [REDACTED] PSP. The access category permitted all of [REDACTED] [REDACTED] employees unauthorized unrestricted physical access to the PSP. On August 12, 2016, upon further review of the noncompliance, [REDACTED] discovered two additional [REDACTED] PSPs that had been inappropriately assigned an access category, which allowed [REDACTED] [REDACTED] employees physical access to the PSPs. Only [REDACTED] [REDACTED] employees were authorized to have such access to the [REDACTED] PSPs.
382. The Alleged Violation started on July 1, 2016, when [REDACTED] granted all of its [REDACTED] employees unauthorized physical access to the newly commissioned PSPs, and ended on August 12, 2016, when [REDACTED] revoked the unauthorized access.

Description of Alleged Violation for [REDACTED]

383. On May 26, 2017 [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] was in violation of CIP-006-6 R1; P1.4. *See* Self-Report, **Attachment 17c**. [REDACTED] had one instance where it did not monitor for unauthorized access through a physical access point into a PSP.
384. On April 20, 2017, [REDACTED] [REDACTED] [REDACTED] conducted a one-off activity to identify and remove physical access monitoring alarms that were not required for CIP-006-6 because they were potentially causing issues with the Physical Access Control Systems (PACSS). [REDACTED] generated a report for this activity and erroneously filtered the alarm point list to include an exit-only

[REDACTED]

door at a [REDACTED] which is a physical access point to the [REDACTED] PSP. The producer of the alarm point list was under the mistaken impression that the door was not a PSP access point and that the alarming and monitoring functions should be disabled.

385. On April 28, 2017, a PACS administrator relied on the erroneous alarm point list and disabled the alarming and monitoring functions for the door. On May 1, 2017, while completing change documentation, a different [REDACTED] PACS administrator discovered the disabled alarming and monitoring functions for the [REDACTED] door and re-enabled such functions.

386. The Alleged Violation started on April 28, 2017, when [REDACTED] disabled alarming and monitoring at the access point, and ended on May 1, 2017, when [REDACTED] re-enabled alarming and monitoring at the access point.

Description of Alleged Violation for [REDACTED]

387. On September 2, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-006-6 R1; P1.8. *See* Self-Report, **Attachment 17d**. [REDACTED] did not maintain complete access logs for one PSP.

388. [REDACTED] policy requires employees with authorized access to a PSP who do not have their employee badge with them to manually complete the PSP visitor access log upon entry into and exit from the PSP. On August 11, 2016, [REDACTED] scheduled a meeting inside a PSP conference room to discuss upcoming outages. At 9:45 a.m., six employees entered the PSP but determined that they needed to use a larger conference room located outside the PSP to accommodate all attendees. At 9:48 a.m., the employees exited the PSP to conduct their meeting in the larger conference room. All employees were authorized to access the PSP; however, one employee did not bring his employee badge to work and did not manually complete the PSP visitor access log upon entry into the PSP. On August 22, 2016, one of the employees who attended the meeting reported the incident.

389. The Alleged Violation started on August 11, 2016, at 9:45, when the employee entered the PSP without first logging the required information in the visitor access logbook, and ended on August 11, 2016, at 9:48, when the employee exited the PSP.



Aggregate Contributing Causes of CIP-006-6 R1 Alleged Violations

390. The primary cause of the CIP-006-6 R1 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient physical access management process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] commissioning process for assigning access categories for substation PSPs did not require a secondary review or approval before assigning categories. Additionally, [REDACTED] process for generating lists for removing physical access monitoring alarms did not include specific steps for generating the lists, and there was no requirement for a secondary review or approval to prevent the disabling of a PSP access point. Moreover, the [REDACTED] employee who left his badge at home was unaware that he was required to manually complete the PSP visitor access log upon entry or exit of a PSP. Additional training, along with stronger internal controls could have helped prevent the Alleged Violations.

Aggregate Risk Statement for CIP-006-6 R1 Alleged Violations

391. The Regions determined that the Alleged Violations posed an aggregate serious and substantial risk⁸⁵ to the reliability of the BPS.⁸⁶ The risk posed was providing the opportunity for unauthorized physical access to BES Cyber Systems (BCSs). Regarding the second Alleged Violation where [REDACTED] granted all [REDACTED] employees physical access to BCSs inside multiple substation PSPs, the PSPs are

[REDACTED]

392. Despite these protective measures, the aggregate risk remains serious and substantial based on several factors. [REDACTED]

[REDACTED]

⁸⁵ Alleged Violation [REDACTED] individually, posed a serious risk to the reliability of the BPS, and [REDACTED] individually, posed a minimal risk.

⁸⁶ CIP-006-6 R1 has a VRF of “Medium” pursuant to the CIP-006-6 Table of Compliance Elements. According to the VSL Matrix, this issue warranted a “Severe” VSL.



[REDACTED]
[REDACTED]
[REDACTED] The Regions determined that [REDACTED] had serious, systemic security and compliance issues across its [REDACTED] functional groups, which resulted in multiple CIP-006 Alleged Violations spanning both version 3 and 6 of the Standard and required [REDACTED] to overhaul its entire CIP compliance program. Because of this, risk for continued noncompliance and compromise to BCSs and CAs dramatically increased. Due to the weaknesses in [REDACTED] CIP compliance program, the Regions anticipate that [REDACTED] will identify additional instances of noncompliance while completing mitigation, which [REDACTED] will report to the Regions. Notwithstanding, [REDACTED] comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that [REDACTED] reports.

Mitigating Actions for CIP-006-6 R1 Alleged Violations

393. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-006-6 R1 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
394. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED]: (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
395. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

P. CIP-006-3c R2 [REDACTED]

396. CIP-006-3c ensures the implementation of a physical security program for the protection of Critical Cyber Assets.
397. CIP-006-3c R2 provides:
- R2.** Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
 - R2.1.** Be protected from unauthorized physical access.
 - R2.2.** Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

Description of Alleged Violation for [REDACTED]

398. On July 23, 2015, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-006-3c R2.2. [REDACTED] failed to afford the protective measures specified in CIP-007-3a R5.1.3 to its Physical Access Control System (PACS). *See* Self-Report, **Attachment 18a**.
399. CIP-007-3a R5.1.3, as applied to CIP-006-3c R2.2, requires [REDACTED] to “ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of ‘need to know’ with respect to functions performed.” On April 1, 2015, [REDACTED] was migrating to a CIP version 5 Compliance Program and evaluating a new Identity Access Management (IAM) tool to assist in identifying Critical Cyber Assets (CCAs), user accounts, and the personnel who have access to those assets. During the evaluation of the IAM tool, [REDACTED] discovered that in 2014, it failed to review [REDACTED] individual PACS user accounts to verify access privileges. The noncompliance affected [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED].
400. The Alleged Violation started on January 1, 2015, when [REDACTED] was required to conduct an annual review of PACS user accounts, and ended on September 30, 2015, when [REDACTED] conducted the 2015 annual review of PACS user accounts.



Description of Alleged Violation for [REDACTED]

401. On October 29, 2015, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-006-3c R2.2 for failing to afford the PACS servers the protective measures specified in CIP-007-3 R5.1.3. *See* Self-Report, **Attachment 18b**.
402. CIP-007-3 R5.1.3, as applied to CIP-006-3c R2.2, requires [REDACTED] to review shared system accounts and verify that access privileges are in accordance with CIP-004-3 R4. CIP-004-3 R4.1 requires [REDACTED] to update its CCA access list within seven calendar days of any change in access rights of personnel. On May 20, 2015, during the second quarter CCA access list review, [REDACTED] discovered that on August 26, 2013, it removed one shared user account and provisioned one individual user account for access to two PACS servers, but did not update its access list until April 2, 2015.
403. The Alleged Violation started on September 3, 2013, seven days after [REDACTED] made changes to the access rights of personnel but failed to update the CCA access list, and ended on April 2, 2015, when [REDACTED] updated the CCA access list to reflect the changes.

Aggregate Contributing Causes of CIP-006-3c R2 Alleged Violations

404. The primary cause of the CIP-006-3c R2 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient electronic access control process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. Regarding the first Alleged Violation, the technical staff lead was unaware that the PACS accounts were also subject to the requirements in CIP-007. There were no internal controls, such as mapping of CIP standards to specific system devices (PACS) to ensure they were protected as required by all applicable standards. Regarding the second Alleged Violation, [REDACTED] utilized an undocumented maintenance process for access review, which produced inconsistent results in the application of the process. Additional training, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violations.



Aggregate Risk Statement for CIP-006-3c R2 Alleged Violations

405. The Regions determined that the Alleged Violations posed an aggregate minimal risk⁸⁷ to the reliability of the BPS.⁸⁸ The risk posed by [REDACTED] failure to annually review the list of individuals with access to the PACS and update the CCA access list was providing the opportunity for an individual who no longer required access to the PACS to retain access permissions and have the ability to physically access CCAs and potentially affect the reliable operations of the BPS. Notwithstanding, regarding the first Alleged Violation, all the individuals who had access to the PACS also had access to CCAs, and [REDACTED] had timely performed the 2014 annual review on the CCA user access list and noted no issues. Furthermore, no changes were made to the PACS user account lists after the completion of the 2015 annual review of the user account list. Additionally, all personnel with PACS access were current on cyber security training and had current personnel risk assessments on file. The PACS reside inside a PSP with monitoring deployed to detect for unauthorized access attempts. Additionally, [REDACTED] has a [REDACTED] [REDACTED] [REDACTED] Regarding the second Alleged Violation, [REDACTED] determined there was no unauthorized access to the PACS servers, and the individuals whose access rights had changed had a business need to the system accounts, were authorized to access such accounts, were current on their cyber security training, and had current PRAs on file.

Mitigating Actions for CIP-006-3c R2 Alleged Violations

406. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-006-3c R2 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
407. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a

⁸⁷ Both Violations, [REDACTED], individually, posed a minimal risk to the reliability of the BPS.

⁸⁸ CIP-006-3c R2.2 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

[REDACTED]

mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

408. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

Q. CIP-006-6 R2 [REDACTED]
[REDACTED]
[REDACTED]

409. CIP-006-6 requires the management of physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

410. CIP-006-6 R2 states:

R2. Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program.

P2.1. Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.

P2.2. Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.

Description of Alleged Violation for [REDACTED]

411. On September 12, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-006-6 R2; P2.1. *See* Self-Report, **Attachment 19a.** [REDACTED] failed to continuously escort a visitor while inside a PSP.

412. On November 17, 2016, during a monthly review of visitor logs, [REDACTED] discovered



one instance where a visitor was not continuously escorted while inside a PSP. On August 8, 2016, a custodial contractor with authorized unescorted physical access to the PSP, who was also an authorized escort, was escorting another visiting custodial contractor in the [REDACTED] [REDACTED] to perform janitorial services. At 10:40 a.m., the authorized escort observed a spill on the break room floor and left the PSP to retrieve a mop bucket from outside the PSP. However, the authorized escort left the visitor unescorted until 10:41 a.m.

413. The Alleged Violation started on August 8, 2016, at 10:40 a.m., when [REDACTED] escort left the visitor unescorted, and ended on August 8, 2016, at 10:41 a.m., when the escort resumed escorting the visitor.

Description of Alleged Violation for [REDACTED]

414. On September 2, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-006-6 R2; P2.2. *See* Self-Report, **Attachment 19b**. [REDACTED] did not maintain complete access logs for one PSP.

415. On August 8, 2016 at 11:15 a.m., a [REDACTED] contractor, who had authorized physical access to the PSP, escorted two visitors into the [REDACTED] [REDACTED]. Upon entry, because the contractor could not locate the visitor access logbook, he questioned the onsite operations staff who told him that the logbook was located outside the PSP at another PSP entrance. As a result, at 11:20 a.m. the contractor left the [REDACTED] with the visitors. However, the contractor failed to retrieve the logbook and document the visitors' entry and exit times within the PSP they visited. Operations staff observed the noncompliance and the hiring manager reported it to [REDACTED] enterprise compliance team.

416. The Alleged Violation started on August 8, 2016, at 11:15 a.m., when the contractor entered the PSP with the two visitors without first documenting the required information in the logbook, and ended on August 8, 2016, at 11:20 a.m., when the contractor and visitors exited the PSP.

Description of Alleged Violation for [REDACTED]

417. During a Compliance Audit conducted from [REDACTED] [REDACTED], the Regions determined that [REDACTED] and [REDACTED] as [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED] were in violation of CIP-006-6 R2; P2.2. *See* PV Summary, **Attachment 19c**. The Alleged Violation involved five instances where [REDACTED] failed to log all required information for visitors who accessed PSPs.

418. In the first four instances, on July, 8, 2016, August 8, 2016, August 17, 2016, and September 10, 2016, [REDACTED] failed to manually log the exit times of visitors who accessed PSPs. In the fifth instance, on September 5, 2016, [REDACTED] failed to manually log the name of the escort for a visitor who accessed a PSP.
419. The Alleged Violation began on July 8, 2016, when, in the first instance, [REDACTED] failed to manually log the exit time of the visitor who accessed a PSP, and ended on September 5, 2016, when, in the fifth instance, [REDACTED] failed to manually log the escort name of a visitor who accessed a PSP.

Description of Alleged Violation for [REDACTED]

420. On September 12, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as [REDACTED] [REDACTED] [REDACTED] and [REDACTED] they were in violation of CIP-006-6 R2; P2.2. See Self-Report, **Attachment 19d**. The Alleged Violation involved two instances where [REDACTED] failed to log all required information for visitors who accessed PSPs.
421. In the first instance, on November 30, 2016, during a monthly review of visitor logs, [REDACTED] discovered that on October 25, 2016, it failed to manually log the exit time of the visitor who accessed a PSP.
422. In the second instance, on December 31, 2016, during a monthly review of visitor logs, [REDACTED] discovered that on November 2, 2016, it failed to manually log the exit time of a visitor who accessed a PSP. In both instances, the visitor was continuously escorted while inside the PSP.
423. The Alleged Violation began on October 25, 2016, when, in the first instance, [REDACTED] failed to manually log the exit time of the visitor who accessed a PSP, and ended on November 2, 2016, when, in the second instance, [REDACTED] failed to manually log the exit time of the visitor who accessed a PSP.

Description of Alleged Violation for [REDACTED]

424. On September 12, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] it was in violation of CIP-006-6 R2; P2.2. See Self-Report, **Attachment 19e**. [REDACTED] failed to log all required information for a visitor who accessed a PSP.
425. On May 11, 2017, during a monthly review of visitor logs, [REDACTED] discovered that on April 18, 2017, at approximately 4:00 p.m., it failed to manually log the exit time of a visitor who accessed a [REDACTED] [REDACTED] PSP.



426. The Alleged Violation started and ended on April 18, 2017, when the visitor exited the PSP and [REDACTED] failed to log the exit time in the logbook.

Description of Alleged Violation for [REDACTED]

427. On December 21, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-006-6 R2; P2.2. See Self-Report, **Attachment 19f**. [REDACTED] failed to log all required information for visitors who accessed PSPs.
428. On September 26, 2017, during a weekly review of PSP electronic visitor logs, [REDACTED] discovered that on September 24, 2017, a [REDACTED] employee made errors in the computerized logging system when logging two visitors who needed access to a [REDACTED] PSP. Specifically, the employee entered his name twice as being the two visitors. After the employee scanned his identification badge, the logging system entered him as the authorized visitor escort. Approximately one hour later, when the employee and visitors exited the PSP, the employee was unable to determine how to log the exit time of the visitors in the logging system.
429. The Alleged Violation began and ended on September 24, 2017, when the escort failed to log in and log out the two PSP visitors.

Description of Alleged Violation for [REDACTED]

430. On December 21, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-006-6 R2; P2.2. See Self-Report, **Attachment 19g**. [REDACTED] failed to log all required information for visitors who accessed a PSP.
431. On October 12, 2017, an authorized escort successfully logged two painters into [REDACTED] newly implemented computerized logging system for access to a [REDACTED] [REDACTED] PSP. At the end of the shift, when the escort and the painters exited the PSP, the escort attempted to sign out the visitors in the logging system. The escort received a “Process Complete” message on the logging system kiosk screen leading the escort to believe that the visitors had been successfully logged out from the PSP. However, the “Process Complete” was only for one-step in the sign-out process, and additional steps were required.
432. Later that same evening, a night shift employee logged into a generation station relay [REDACTED] PSP and noticed that the two painters were still logged in as being inside the PSP. The night shift employee realized the breakdown in the sign-out process and reported the matter to appropriate personnel.

433. The Alleged Violation began and ended on October 12, 2017, when the escort failed to complete the log out process for the two visitors.

Description of Alleged Violation for [REDACTED]

434. On January 5, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-006-6 R2; P2.2. *See* Self-Report, **Attachment 19h**. [REDACTED] failed to log all required information for a visitor who accessed a PSP.
435. On October 21, 2017, a contractor with unescorted access privileges was escorting a visitor inside a PSP. Although the date and time of the visitor's initial entry into the PSP were logged, the date and time the visitor exited the PSP was not logged.
436. The Alleged Violation started and ended on October 21, 2017, when the escort failed to log the exit date and time of the visitor.

Aggregate Contributing Causes of CIP-006-6 R2 Alleged Violations

437. The primary cause of the CIP-006-6 R2 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient electronic access control process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. For one of the eight Alleged Violations, instead of having a PSP logbook at each individual PSP, two PSPs shared the same logbook. Thus, the logbook associated with the noncompliance was located at a different PSP. For the remaining seven Alleged Violations, additional training could have helped prevent the Alleged Violations. For instance, for two of the Alleged Violations, the employee had trouble figuring out how to log visitors in/out using the newly implemented computerized logging system. Additionally, due to the number of instances, additional training to reinforce [REDACTED] visitor control program was necessary to help prevent the Alleged Violations.



Aggregate Risk Statement for CIP-006-6 R2 Alleged Violations

438. The Regions determined that the Alleged Violations posed an aggregate moderate⁸⁹ risk to the reliability of the BPS based on the following factors.⁹⁰ The risk posed by [REDACTED] failure to completely document visitor PSP logbooks and continuously escort visitors while inside PSPs was providing the opportunity for unauthorized physical access to [REDACTED] BES Cyber Assets without [REDACTED] knowledge. However, for 12 of the 13 instances associated with the eight Alleged Violations, the visitors were continuously escorted while inside the PSP. For the one instance where the visitor was not escorted, the duration was only one minute, when the escort left to retrieve a mop and bucket after he observed a spill on the floor. Notwithstanding, the aggregate moderate risk is appropriate because from July 8, 2016 to October 21, 2017, there were 13 separate instances of noncompliance.

Mitigating Actions for CIP-006-6 R2 Alleged Violations

439. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-006-6 R2 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
440. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
441. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED]

⁸⁹ All CIP-006-6 R2 Alleged Violations, individually, posed a minimal risk to the reliability of the BPS.

⁹⁰ CIP-006-6 R2 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

completion of the Mitigation Activities and promptly report its successful completion to NERC.

R. CIP-006-3c R4 [REDACTED]

442. CIP-006-3c ensures the implementation of a physical security program for the protection of Critical Cyber Assets.

443. CIP-006-3c R4 provides:

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

Description of Alleged Violation and Risk Assessment for [REDACTED]

444. On June 16, 2015, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-006-3c R4. *See* Self-Report, **Attachment 20a**. [REDACTED] failed to implement operational or procedural controls to manage physical access to a Physical Security Perimeter (PSP).

445. On March 31, 2015, at 8:15 a.m., a [REDACTED] [REDACTED] plant technician entered a [REDACTED] [REDACTED] (a Critical Asset) to conduct a review of the fire protection plan for the site. The technician called and advised [REDACTED] security staff that personnel would be in the [REDACTED] but would not need to access the [REDACTED] [REDACTED], which is a PSP. At 8:40 a.m., the [REDACTED] security monitoring group received an unauthorized access attempt alert, followed by a forced entry alarm for the



██████████. At 8:41 a.m., ██████ security contacted the technician on site and instructed the technician to leave the ██████████ immediately because the technician did not have authorized unescorted access permissions for the PSP. The technician left the PSP at 8:42 a.m. ██████ ██████ had an override key for the ██████████ ██████████ in the event an emergency at the site required immediate access. The technician received the override key from the ██████ ██████ ██████████ in error, and used the key to gain access to the ██████████ PSP.

- 446. The primary cause was insufficient training. ██████ staff lacked an understanding concerning the CIP controls implemented and how the ██████ ██████ managed the override key program.
- 447. The Alleged Violation began on March 31, 2015, at 8:40 a.m., when the unauthorized ██████ technician accessed the PSP, and ended on March 31, 2015, at 8:42 a.m., when the ██████ technician exited the PSP.
- 448. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the BPS.⁹¹ The risk posed was providing the opportunity for unauthorized physical access to CCAs inside the PSP, which could have led to the manipulation or degradation of CCA operational functionality. Notwithstanding, the risk was mitigated because the duration of the noncompliance was limited to two minutes, and the use of the override key resulted in an immediate “forced entry” alarm to the security-monitoring group, prompting an immediate investigation and mitigation of the potential risk.

Mitigating Actions for CIP-006-3c R4 Alleged Violations

- 449. On September 11, 2018, ██████ submitted to ██████ its final Mitigation Activities to address the CIP-006-3c R4 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, ██████ accepted the Mitigation Activities.
- 450. In the Mitigation Activities, ██████ committed to take the following actions by ██████ ██████████ (i) revise its overarching corporate ██████████ program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each ██████ business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the ██████████ program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and

⁹¹ CIP-006-3c R4 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

[REDACTED]

(v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

451. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

S. CIP-006-3c R5 [REDACTED]
[REDACTED]

452. CIP-006 ensures that a Responsible Entity implements a physical security program for the protection of Critical Cyber Assets.

453. CIP-006-3c R5 provides:

R5. Monitoring Physical Access—The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

Description of Alleged Violation for [REDACTED]

454. On July 14, 2015, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-006-3c R5. *See Self-Report, Attachment 21a.* [REDACTED] failed to immediately review unauthorized physical access attempts at a Physical Security Perimeter (PSP).



455. On April 8, 2015, during the review of a report containing all unauthorized physical access attempts to PSPs, [REDACTED] discovered that the offsite centralized security monitoring staff failed to contact impacted site personnel regarding multiple unauthorized access attempts to a [REDACTED] PSP on April 7, 2015. Specifically, a [REDACTED] employee, who did not have authorized access to the PSP, made seven unauthorized physical access attempts to the PSP in less than one minute. [REDACTED] operational procedures require the offsite centralized security monitoring staff to contact the impacted site personnel upon detection of [REDACTED] [REDACTED] However, the security monitoring staff failed to contact appropriate personnel so that the unauthorized access attempts could be investigated.
456. The Alleged Violation started on April 7, 2015, when [REDACTED] failed to immediately review unauthorized access attempts at the PSP, and ended on April 8, 2015, when [REDACTED] reviewed the unauthorized access attempts to the PSP.

Description of Alleged Violation for [REDACTED]

457. On March 1, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-006-3c R5. *See* Self-Report, **Attachment 21b**. [REDACTED] failed to continuously monitor physical access at two access points to a PSP.
458. On December 29, 2015, during an internal assessment of its alarming functions, [REDACTED] discovered that two exit only doors at one of its [REDACTED] [REDACTED] were not sending notifications to the security command center alerting them each time one of these doors were opened. The [REDACTED] created an emergency work order to have the vendor repair the system, which was completed on December 31, 2015. The vendor determined that the [REDACTED] that the door alarm devices connected to was locked up and not functioning. The vendor reset the [REDACTED] and synchronized the connection with the Physical Access Control System (PACS) for both doors.
459. On January 2, 2016, [REDACTED] restored the monitoring and alarming functionality of the two PSP exit doors. [REDACTED] reviewed the door logs and determined that the [REDACTED] locked up on December 16, 2016.
460. The Alleged Violation started on December 16, 2015, when [REDACTED] [REDACTED] device locked up thereby stopping the monitoring and alarming functionality for the two PSP doors, and ended on January 2, 2016, when [REDACTED] repaired the [REDACTED] and monitoring and alarming functionalities for the two PSP doors resumed.



Description of Alleged Violation for [REDACTED]

- 461. On April 19, 2016, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-006-3c R5. *See* Self-Report, **Attachment 21c**. [REDACTED] failed to immediately review unauthorized physical access attempts at a PSP.
- 462. On February 15, 2016, at 8:56 a.m., an operator at a control center received an alarm for an unauthorized physical access attempt from a substation PSP badge reader. The supervisor who received the alarm mistakenly placed the alarm in [REDACTED] mode on a drop-down menu in the software, which is used to acknowledge alarms. Once the alarm went into [REDACTED] mode, no further alarms for this particular access point would show on the computer screen viewed by the operators. On February 18, 2016, at 1:47 p.m., another employee noticed that the alarms were in [REDACTED]'s mode. [REDACTED] performed an analysis by querying the PACS system alarm history and found four additional alarms that were not issued related to the same incident because the initial alarm had been placed in [REDACTED] mode.
- 463. The Alleged Violation started on February 15, 2016, when [REDACTED] failed to immediately review an unauthorized access attempt at the PSP, and ended on February 18, 2016, when [REDACTED] reviewed the unauthorized access attempt.

Description of Alleged Violation for [REDACTED]

- 464. On August 11, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-006-3c R5. *See* Self-Report, **Attachment 21d**. [REDACTED] failed to continuously monitor physical access at two access points to a PSP.
- 465. On June 28, 2016, while conducting its bi-annual physical security maintenance and testing inspection of a control center PSP, [REDACTED] discovered that two exit only doors at the PSP were not sending notifications to the security command center alerting them each time one of these doors were opened. [REDACTED] immediately contacted its vendor for support. The vendor determined that a [REDACTED] employee failed to configure the PACS in alignment with the installed vendor software, which prevented the notifications from being sent to the security command center. [REDACTED] discovered that the doors had not alarmed since January 2, 2016, when they were last tested.
- 466. The Alleged Violation started on January 3, 2016, when the monitoring and alarming functionality for the two PSP doors ceased, and ended on June 29, 2016, when [REDACTED] reconfigured its PACS and monitoring and alarming functionalities for the two PSP doors resumed.

Description of Alleged Violation for [REDACTED]

467. On August 11, 2016,⁹² [REDACTED] submitted two Self-Reports to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED] they were in violation of CIP-006-3c R5. *See* Self-Reports, **Attachment 21e**. This Alleged Violation involved two instances where [REDACTED] failed to continuously monitor physical access to PSPs.
468. In the first instance, on April 11, 2016, [REDACTED] security personnel at its [REDACTED] noticed a delay between the time the PACS issued an alarm and the time the alarm appeared on the [REDACTED] monitoring consoles. On April 14, 2016, the [REDACTED] senior management initiated an internal investigation. On April 18, 2016, [REDACTED] reviewed the March 15, 2016 through April 15, 2016 system logs and determined that [REDACTED] PACS alarms were either delayed and/or not acknowledged.
469. In the second instance, on May 31, 2016 at approximately 2:20 p.m., the [REDACTED] lost power and failed over the PACS applications to a secondary site, which allowed [REDACTED] to continue to monitor PACS alarms. On June 1, 2016, [REDACTED] discovered that there was a performance issue on the issuance of the PACS alarms at its secondary location. The PACS queued the alarms and failed to forward the alarms to the [REDACTED] for acknowledgement or action. In an attempt to fix the alerting issue, the [REDACTED] [REDACTED] [REDACTED] initiated a change management ticket to fail the [REDACTED] systems back over to the primary location. [REDACTED] Information Technology (IT) personnel failed over PACS alerting operations back to the primary [REDACTED] Later that day, [REDACTED] vendor instructed the IT personnel to delete logs and alerts to alleviate issues with the alarm queue. [REDACTED] was still experiencing issues with the [REDACTED] receiving alerts, so IT personnel decided to failover the application back to secondary site. At approximately 8:32 p.m., [REDACTED] restored the alarming and alerting functionality while operating at a secondary site.
470. The Alleged Violation began on October 26, 2015, when [REDACTED] began deploying the new PACS, and ended on August 8, 2016, when [REDACTED] commissioned a new server and implemented applicable patches.

Aggregate Contributing Causes of CIP-006-3c R5 Alleged Violations

471. The primary cause of the CIP-006-3c R5 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient physical access management

⁹² One August 11, 2016 self-reported noncompliance was assigned [REDACTED] Tracking Number [REDACTED], but was administratively dismissed and consolidated with [REDACTED] on August 8, 2016. This noncompliance involves [REDACTED] for its [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED] function.

[REDACTED]

process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] did not have controls in place that would prevent operators and supervisors from mistakenly placing alarms into bypass mode, which resulted in [REDACTED] personnel not responding to subsequent alarms. Additionally, [REDACTED] process did not include steps for validating door alarms when configuring the PACS and there were no internal controls to verify that the doors were monitoring for unauthorized access attempts to the PSP. Furthermore, when deploying new PACS, [REDACTED] performed testing on the individual installations (e.g. door controllers) and steadily increased the addition of PACS devices; however, [REDACTED] did not anticipate the overall system impact when all the devices were deployed and configured within the new PACS. The software would not allow multiple alarms to be simultaneously processed. Moreover, when a power failure occurred at the primary [REDACTED] preventing PACS alarms from being issued, [REDACTED] was not prepared on how to quickly address and correct the alarming issue.

Aggregate Risk Statement for CIP-006-3c R5 Alleged Violations

472. The Regions determined that the Alleged Violations posed an aggregate serious and substantial risk⁹³ to the reliability of Bulk Power System.⁹⁴ The risk posed by the CIP-006-3c R5 Alleged Violations was providing the opportunity for undetected compromise to CCAs and [REDACTED] inability to respond to potential risks due to lack of situational awareness. However, [REDACTED] implemented the following protective measures. For two of the Alleged Violations, the PSP doors that did not alarm each time one of the doors opened, the doors were for exiting the PSP. As a result, there is not a badge reader outside the PSP doors; therefore, badge access to the PSP from the outside is not possible. Additionally, the facility was locked and secured at all times and resides within a fenced perimeter with access control at the entry points to the perimeter.
473. Despite these protective measures, the aggregate risk remains serious and substantial based on several factors. Regarding the last Alleged Violation where PACS alarms were not being issued or investigated, the noncompliance affected all [REDACTED] of [REDACTED] function groups, and [REDACTED] failure to alert on almost [REDACTED] PSP alarms over an approximate six-month period could have resulted in unauthorized

⁹³ Alleged Violation [REDACTED] individually, posed a serious risk to the reliability of the BPS, [REDACTED] [REDACTED] [REDACTED] individually, posed a moderate risk, and [REDACTED] individually, posed a minimal risk.

⁹⁴ CIP-006-3c R5 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

■■■■■ individuals repeatedly accessing the PSP without ■■■■■ knowledge, which could have caused physical damage to critical assets. The Regions determined that ■■■■■ had serious, systemic security and compliance issues across its ■■■■■ functional groups, which required ■■■■■ to overhaul its entire CIP compliance program. Because of this, the risk for continued noncompliance and compromise to BES Cyber Systems and Cyber Assets dramatically increased. Due to the weaknesses in ■■■■■ CIP compliance program, the Regions anticipate that ■■■■■ will identify additional instances of noncompliance while completing mitigation, which ■■■■■ will report to the Regions. Notwithstanding, ■■■■■ comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that ■■■■■ reports.

Mitigating Actions for CIP-006-3c R5 Alleged Violations

474. On September 11, 2018, ■■■■■ submitted to ■■■■■ its final Mitigation Activities to address the CIP-006-3c R5 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, ■■■■■ accepted the Mitigation Activities.
475. In the Mitigation Activities, ■■■■■ committed to take the following actions by ■■■■■
■■■■■ (i) revise its overarching corporate ■■■■■ program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each ■■■■■ business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the ■■■■■ program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) ■■■■■ will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
476. Upon completion of these Mitigation Activities, ■■■■■ shall promptly provide evidence supporting the completion to ■■■■■ ■■■■■ will verify ■■■■■ completion of the Mitigation Activities and promptly report its successful completion to NERC.

T. CIP-007-3a R1 [REDACTED]

477. CIP-007 ensures that Responsible Entities define methods, processes, and procedures for securing those systems determined to be CCAs, as well as the non-critical Cyber Assets within the ESP.
478. CIP-007-3a R1 provides:
- R1.** Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
 - R1.1.** The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.
 - R1.2.** The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
 - R1.3.** The Responsible Entity shall document test results.

Description of Alleged Violation for [REDACTED]

479. During a Compliance Audit conducted [REDACTED], the Regions determined that [REDACTED] as a [REDACTED] [REDACTED] and [REDACTED] was in violation of CIP-007-3a R1.1, R1.2, and R1.3. See PV Summary, **Attachment 22a**. This Alleged Violation involved multiple instances where [REDACTED] failed to adhere to its cyber security testing procedures.
480. [REDACTED] failed to implement a cyber security testing plan in a manner that minimizes adverse effects on the production system or its operation per R1.1. During the transition to the CIP version 5 testing program, [REDACTED] implemented changes to the testing environment but did not properly document the differences between the production and the test environments. As a result, testing that occurred would not adequately reflect the production environment.
481. Because [REDACTED] failed to document the difference between the production and testing environments, it did not perform three subsequent instances of testing of implemented changes to [REDACTED] Critical Cyber Assets (CCAs) in a manner that reflected the production environment as required by R1.2. Specifically, [REDACTED] performed deficient testing on software upgrades on September 3, 2015 for [REDACTED] CCAs, on October 23, 2015 for [REDACTED] CCA, and on October 27, 2015, for [REDACTED] CCA.

Moreover, [REDACTED] failed to document the results of these deficient tests per R1.3. [REDACTED] utilizes an automated configuration management tool that runs daily reports. For each of these testing instances, [REDACTED] discovered the issue the day following each test.

482. The Alleged Violation started on September 3, 2015, the earliest date [REDACTED] performed the deficient testing on software upgrades, and ended on May 24, 2016, when [REDACTED] successfully completed its change management process for the devices involved.

Description of Alleged Violation for [REDACTED]

483. On August 4, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-007-3a R1.1. See Self-Report, **Attachment 22b**. Also, on September 2, 2016, [REDACTED] submitted two Self-Reports to [REDACTED] stating that as [REDACTED] they were in violation of CIP-007-3a R1. See Self-Reports, **Attachments 22c⁹⁵ and 22d.⁹⁶** These Alleged Violations involved five instances where [REDACTED] implemented changes to existing Cyber Assets (CAs) and CCAs within an Electronic Security Perimeter (ESP) without first testing the changes to ensure they would not adversely affect existing cyber security controls.
484. In the first instance, on March 14, 2016, a [REDACTED] [REDACTED] team subject matter expert (SME) submitted a change management ticket to add software to [REDACTED] CAs, [REDACTED] of which were CCAs. On March 25, 2016, the SME installed the software on the CAs and CCAs without performing the required testing to ensure the changes would not adversely affect the existing cyber security controls.
485. On June 1, 2016, the [REDACTED] performed its daily review of NERC CIP CA/CCA changes and discovered the change management ticket was in a “work in progress” status, which prevented the workflow from starting the cyber security control testing process. On June 10, 2016, the SME created a new change management ticket to complete the cyber security testing. On June 22, 2016, [REDACTED] completed the cyber security testing and did not identify any issues. However, [REDACTED] extended the testing through July 20, 2016, because it required the SME to validate the results in diverse environments across [REDACTED] control centers.

⁹⁵ This self-reported noncompliance involved three instances and was assigned [REDACTED] Tracking Number [REDACTED] [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on September 20, 2016. This noncompliance involves [REDACTED] for its [REDACTED] function.

⁹⁶ This September 2, 2016 self-reported noncompliance was assigned [REDACTED] Tracking Number [REDACTED] but was administratively dismissed and consolidated with [REDACTED] on February 28, 2017. This noncompliance involves [REDACTED] for its [REDACTED] function.



486. In the second instance, on April 18, 2016, ██████ submitted a change management ticket to begin an operating system upgrade to an electronic access control and monitoring system (EACMS). The ██████ SME did not categorize the device as a NERC CIP device in the change management ticket. Therefore, the software did not initiate the testing workflow. On May 16, 2016, the SME completed the operating system upgrade. On May 17, 2016, the automated change control monitoring software detected an untested change to the EACM, and the SME generated a new change management ticket indicating that the asset was a NERC CIP device. On May 18, 2016, ██████ completed the required cyber security controls testing and did not discover any issues.
487. On August 10 and 11, 2016, ██████ performed site-specific CIP CA walk downs to ensure it had implemented the appropriate protections on its identified CIP assets and discovered instances 3-5. In the third instance, on July 22, 2015, ██████ replaced two CCAs at a ██████ without conducting a cyber security control test. In addition, the employee did not update the device list software or communicate the changes to the engineering department. As a result, ██████ did not update the changes in its database, which was used to track information of the CCAs.
488. In the fourth instance, in May 2015, ██████ performed a firmware upgrade to a programmable automation controller without conducting cyber security testing on the asset prior to implementation. In addition, upon completion of the firmware upgrade, the SME did not update the device list software or communicate the changes to the engineering department.
489. In the fifth instance, on April 30, 2015, ██████ installed a new CCA for an upgrade on a ██████ without conducting a cyber security control test or maintaining sufficient change management documentation. In addition, upon completion of the upgrade, the SME did not update the device list software or communicate the changes to the engineering department.
490. The Alleged Violation started on April 30, 2015, when, in the fifth instance, ██████ installed a new device without performing a cyber security controls test, and ended on August 31, 2016, when ██████ completed the cyber security controls test.

Description of Alleged Violation for ██████

491. On August 11, 2017, ██████ on behalf of ██████ submitted a Self-Report to ██████ stating that, as a ██████ and ██████ it was in violation of CIP-007-3a R1.1.⁹⁷ See Self-Report, **Attachment 22e**. ██████ failed to implement its cyber security test

⁹⁷ The Alleged Violation was self-reported under CIP-007-3a R1.3; however, the Regions determined that R1.1 is the applicable requirement.

[REDACTED]

procedures for one CA.

492. On June 14, 2017, while performing a CIP version 5 Cyber Vulnerability Assessment, [REDACTED] discovered that on May 9, 2016, it deployed a port server, which allows access to the serial port of another device over [REDACTED] Protocol/Internet Protocol, inside an ESP without first testing the server to ensure it did not adversely affect existing cyber security controls. When initially processing the change management system ticket for the new server, an employee mistakenly closed the ticket without setting the proper classification for the server. Without the proper classification, the security controls testing system could not automatically execute the CIP testing workflows to ensure that required testing occurred.
493. The Alleged Violation started on May 9, 2016, when [REDACTED] failed to conduct a cyber security test before deploying the port server, and ended on July 31, 2017, when the server was tested.

Aggregate Contributing Causes for CIP-007-3a R1 Alleged Violations

494. The primary cause of the CIP-007-3a R1 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] cyber security testing process did not clearly define the roles and responsibilities for the transition from CIP version 3 to version 5. Additional training on the new cyber security testing software, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violations.

Aggregate Risk Assessment for CIP-007-3a R1 Alleged Violations

495. The Regions determined that the CIP-007-3a R1 Alleged Violations posed an aggregate serious or substantial risk⁹⁸ to the reliability of the Bulk Power System.⁹⁹ The risk posed by [REDACTED] failure to adhere to its cyber security test procedures was providing the opportunity for the installation of new CCAs and significant changes to existing CCAs within the ESP that could adversely affect existing cyber security controls. However, [REDACTED] did implement a tool that ran daily report, which allowed it to promptly discover some of the instances. Additionally, [REDACTED] maintained the CCAs within a secured ESP inside an established PSP, and [REDACTED] deployed a

⁹⁸ [REDACTED], individually, posed a serious risk to the reliability of the BPS, and [REDACTED] and [REDACTED], individually, posed a moderate risk.

⁹⁹ CIP-007-3a R1 has a VRF of “Medium” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

network based intrusion detection system to detect anomalous activities of CCAs.

496. Despite these protective measures, the aggregate risk remains serious and substantial based on several factors. The three Alleged Violations collectively involved implemented system upgrades to ██████████ CCAs without prior testing. Additionally, in the first instance in the second Alleged Violation, ██████████ implemented software to ██████████ CAs, ██████████ of which were CCAs, without prior testing. The Regions determined that ██████████ had serious, systemic security and compliance issues across its ██████████ functional groups, which required ██████████ to overhaul its entire CIP compliance program. Because of this, the risk for continued noncompliance and compromise to BES Cyber Systems and CAs dramatically increased. Due to the weaknesses in ██████████ CIP compliance program, the Regions anticipate that ██████████ will identify additional instances of noncompliance while completing mitigation, which ██████████ will report to the Regions. Notwithstanding, ██████████ comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that ██████████ reports.

Mitigating Actions for CIP-007-3a R1 Alleged Violations

497. On September 11, 2018, ██████████ submitted to ██████████ its final Mitigation Activities to address the CIP-007-3a R1 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, ██████████ accepted the Mitigation Activities.
498. In the Mitigation Activities, ██████████ committed to take the following actions by ██████████ ██████████: (i) revise its overarching corporate ██████████ program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each ██████████ business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the ██████████ program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) ██████████ will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
499. Upon completion of these Mitigation Activities, ██████████ shall promptly provide evidence supporting the completion to ██████████ ██████████ will verify ██████████ completion of the Mitigation Activities and promptly report its successful completion to NERC.

U. CIP-007-6 R1 [REDACTED]

500. 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.
501. CIP-007-6 R1 provides in relevant part:
- R1.** 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 R1 – Ports and Services.
- P1.1.** Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.

Description of Alleged Violation and Risk Statement for [REDACTED]

502. On August 31, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation CIP-007-6 R1; P1.1.¹⁰⁰ See **Attachment 23a**. On April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as [REDACTED] [REDACTED] and [REDACTED] they were in violation CIP-007-6 R1; P1.1.¹⁰¹ See Self-Report, **Attachment 23b**. On January 23, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation CIP-007-6 R1; P1.1.¹⁰² See Self-Report, **Attachment 23c**.
503. In the first instance, on July 20, 2016, during a quarterly Cyber Asset (CA) list review, [REDACTED] discovered that it had not identified three Electronic Access Control and Monitoring System (EACMS) devices (security information and event management CAs), which were deployed outside the Electronic Security Perimeter (ESP) and each protected a [REDACTED]. As a result, [REDACTED] failed implement its security patch management program on these EACMSs as required by CIP-007-

¹⁰⁰ This noncompliance was self-reported under CIP-002-5.1 R1.2. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-007-6 R1 is the applicable Standard and Requirement.

¹⁰¹ This noncompliance was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-007-6 R1 is the applicable Standard and Requirement.

¹⁰² This noncompliance was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-007-6 R1 is the applicable Standard and Requirement.



6 R1.

504. This instance affected [REDACTED]
[REDACTED]
505. In the second self-reported instance of noncompliance, during a CA categorization review on January 5, 2017, [REDACTED] that it had not identified three [REDACTED] as EACMSs. As a result, [REDACTED] failed to ensure that only logical network accessible ports that were needed were enabled per CIP-007-6 R1; P1.1.
506. This instance affected a total of [REDACTED]
[REDACTED]
507. In the third self-reported instance of noncompliance, as part of an extent of condition assessment on November 15, 2017, [REDACTED] determined that it had not identified nine servers as EACMSs. As a result, [REDACTED] failed to ensure that only logical network accessible ports that were needed were enabled per CIP-007-6 R1; P1.1.
508. This instance affected a total of [REDACTED]
[REDACTED]
509. The primary cause was [REDACTED] implementation of insufficient training on identifying in-scope EACMSs.
510. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED], the date [REDACTED] committed to complete its Mitigation Plan.
511. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the Bulk Power System (BPS).¹⁰³ [REDACTED] failure to enable only logical network accessible ports that have been determined to be needed and to protect against the use of unnecessary physical input/output ports for these EACMS, could leave these devices vulnerable to an attack, which could negatively affect BPS reliability. However, [REDACTED] deployed the EACMSs behind a firewall, logged events to detect malicious code, as well as successful and failed login attempts, and changed known default password per Cyber Asset capability and enforced password complexity. [REDACTED] also deployed methods to enforce authentication of interactive user access.

Mitigating Actions for CIP-007-6 R1 Alleged Violations

¹⁰³ CIP-007-6 R1 has a VRF of “Medium” pursuant to CIP-007-6 Table of Compliance Elements. According to the VSL Matrix, this issue warranted a “High” VSL.



512. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-007-6 R1 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
513. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
514. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

V. CIP-007-6 R2 [REDACTED]
[REDACTED]

515. 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.
516. CIP-007-6 R2 provides:
- 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.
- P2.1.** 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.

P2.2 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.

P2.3. 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.

P2.4. 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 Alleged Violation for [REDACTED]

517. On [REDACTED] [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-007-6 R2; P2.2. *See* Self-Report, **Attachment 24a.** [REDACTED] did not evaluate security patches for an application installed on eight BES Cyber Assets (BCAs).
518. In [REDACTED] while preparing evidence for an upcoming Compliance Audit, [REDACTED] discovered that it failed to monitor for vendor security patches and vulnerability notifications for an application on [REDACTED] BCAs.
519. The Alleged Violation began on July 1, 2016, the date the Standard became mandatory and enforceable and [REDACTED] failed to conduct a patch evaluation for the BCAs, and ended on December 22, 2017, when [REDACTED] began monitoring for patches for the BCAs.

Description of Alleged Violation for [REDACTED]

520. On August 14, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that as a [REDACTED] [REDACTED] was in violation of CIP-007-6 R2; P2.2. *See* Self-Report, **Attachment 24b.** [REDACTED] failed to timely conduct two security patch evaluations.
521. On both July 27, 2016 and August 26, 2016, [REDACTED] patch vendor submitted a total of two relay security patches to [REDACTED] for applicability evaluations. On August 19, 2016, and September 6, 2016, the employee who received the vendor patch notifications sent emails to personnel responsible for conducting the evaluations and requested that evaluations be conducted. However, [REDACTED] did not conduct the patch evaluations until October 6, 2016. [REDACTED] determined that both patches were

[REDACTED]

not applicable; therefore, [REDACTED] did not apply them.

522. The Alleged Violation started on September 1, 2016, the earliest date [REDACTED] was required to conduct a patch evaluation, and ended on October 6, 2016, when [REDACTED] conducted evaluations for both patches.

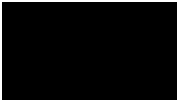
Description of Alleged Violation for [REDACTED]

523. On September 5, 2017, [REDACTED] submitted a Self-Report to [REDACTED] behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-007-6 R2; P.2.2.¹⁰⁴ See Self-Report, **Attachment 24c**. [REDACTED] failed to timely conduct patch evaluations for [REDACTED] security patches.
524. On April 24, 2017, while performing security patch evaluations, [REDACTED] discovered that it had not performed security patch evaluations for [REDACTED] patches relating to a [REDACTED] control system, specifically, Electronic Access Control and Monitoring Systems (EACMSs) and [REDACTED] BCAs. The patches were released on February 6, 2017, but they were not evaluated until April 26, 2017.
525. The Alleged Violation started on March 7, 2017, when [REDACTED] was required to conduct the patch evaluations, and ended on April 26, 2017, when [REDACTED] conducted the patch evaluations.

Description of Alleged Violation for [REDACTED]

526. On September 12, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation of CIP-007-6 R2; P2.2. See Self-Report, **Attachment 24d**. [REDACTED] failed to timely conduct patch evaluations for five security patches.
527. On April 28, 2017, [REDACTED] notified Responsible Entities, including [REDACTED] of a certain line relay security patch release by a vendor, which occurred on April 6, 2017. [REDACTED] was unaware of the patch release because the vendor's website that [REDACTED] monitored for patch releases had moved the information to a new location on the website. [REDACTED] investigated and discovered that it did not know about [REDACTED] security patches that the vendor released beginning August 9, 2016 through April 6, 2017. On August 23, 2017, [REDACTED] evaluated the missed patches and determined none were applicable.
528. The Alleged Violation started on September 14, 2016, the earliest date that [REDACTED] was required to conduct the patch evaluation, and ended on August 23, 2017, when

¹⁰⁴ [REDACTED] also self-reported noncompliance with R2.3; however, the Regions determined that R2.3 was not applicable to this Alleged Violation.



533. In the third instance, during a CA categorization review on January 5, 2017, [REDACTED] discovered that it had not identified [REDACTED] [REDACTED] as EACMSs. As a result, [REDACTED] failed implement its security patch management program on these EACMSs as required by CIP-007-6 R2; P2.1; P2.2; P2.3; and P2.4.
534. This instance affected [REDACTED] [REDACTED] [REDACTED]
535. In the fourth instance, as part of an extent of condition assessment on November 15, 2017, [REDACTED] determined that it had not identified [REDACTED] servers as EACMSs. As a result, [REDACTED] failed implement its security patch management program on these EACMSs as required by CIP-007-6 R2; P2.3; and P2.4.
536. This instance affected [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
537. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED], the date [REDACTED] committed to complete its Mitigation Plan.

Aggregate Contributing Causes for CIP-007-6 R2 Alleged Violations

538. The primary cause of the CIP-007-6 R2 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient security patch management process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process to help ensure that the process was sufficient and followed. The process did not clearly define the individual roles and responsibilities of [REDACTED] personnel. For instance, the process did not address all devices to be tracked, and as a result, not all devices were included in [REDACTED] automated tracking management program. Additionally, [REDACTED] discovered that many [REDACTED] personnel responsible for patch evaluations were neither familiar with the process nor trained on the process. Further, for the instances where [REDACTED] failed to identify EACMSs, [REDACTED] personnel lacked adequate training to identify in-scope EACMSs. Additional training, along with clearer instructions for completing tasks, could have helped prevent the Alleged Violations.

Aggregate Risk Statement for CIP-007-6 R2 Alleged Violations

539. The Regions determined that the Alleged Violation posed an aggregate serious and

substantial risk¹⁰⁸ to the reliability of the Bulk Power System.¹⁰⁹ The risk posed by [REDACTED] failure to timely assess and implement applicable patches was providing the opportunity for infiltration of unauthorized network traffic into ESPs. However, for the second Alleged Violation where two relay patches were not timely evaluated, the evaluations were late by only six days for one patch and 36 days for the other patch, and the patches were deemed not applicable. Regarding the fourth Alleged Violation where [REDACTED] was unaware of the [REDACTED] vendor security patches because patch releases were moved to a new location on the vendor website, [REDACTED] evaluated the patches and deemed them not to be applicable. For all instances, except for those involving the identification of EACMSs, the BCAs were within an ESP. Also, for all Alleged Violations, the BCAs were inside a PSP, and [REDACTED] EMS and associated CAs were monitoring and logging cyber security incidents, physical intrusion, and loss of functionality.

540. Notwithstanding, the aggregate risk remains serious and substantial because [REDACTED] did not include the multiple devices on its tracking management tool or train staff on the process, and in three separate instances, it failed to identify devices as EACMSs, and therefore, did not provide the protective measures required by CIP-007-6 R2.

Mitigating Actions for CIP-007-6 R2 Alleged Violations

541. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-007-6 R2 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
542. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed

¹⁰⁸ All Alleged Violations, individually, posed a moderate risk to the reliability of the BPS.

¹⁰⁹ CIP-007-6 P2.3 has a VRF of “Medium” pursuant to CIP-007-6 Table of Compliance Elements. According to the VSL Matrix, this issue warranted a “High” VSL.

[REDACTED]

in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

543. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

W. CIP-007-3a R3 [REDACTED]

544. CIP-007 ensures that Responsible Entities define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter.

545. CIP-007-3a R3 provides:

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

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 Alleged Violation for [REDACTED]

546. On April 13, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation of CIP-007-3a R3.1. *See* Self-Report, **Attachment 25a**. [REDACTED] failed to assess patches within 30 days of release for multiple Cyber Assets (CAs).
547. On January 19, 2016, [REDACTED] conducted an internal spot check of its security patch-monitoring program for the [REDACTED] for the previous four months. [REDACTED] discovered that it failed to assess [REDACTED] security patches within 30 days of availability.

548. The Alleged Violation started on September 24, 2015, when [REDACTED] failed to assess its first available patch within 30 days of release, and ended on February 26, 2016, when [REDACTED] assessed all available patches.

Description of Alleged Violation for [REDACTED]

549. On April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-007-3a R3. *See Self-Report, Attachment 25b.* [REDACTED] did not implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all CAs within an Electronic Security Perimeter (ESP).
550. On August 15, 2015, [REDACTED] transferred the responsibility of monitoring for applicable security patches and security vulnerabilities for [REDACTED] switches from its [REDACTED] to its [REDACTED]. However, the [REDACTED] was still responsible for installing applicable patches once the [REDACTED] [REDACTED] notified them of applicable patches that needed to be installed. In [REDACTED] [REDACTED], during audit preparation review sessions, [REDACTED] discovered that since the transfer of responsibility, the [REDACTED] [REDACTED] failed to monitor vendor security patches and vulnerability notifications. [REDACTED] identified [REDACTED] security vulnerabilities applicable to the [REDACTED] switches. [REDACTED]
[REDACTED]
[REDACTED] [REDACTED] [REDACTED]
[REDACTED]

551. The Alleged Violation started on August 15, 2015, when [REDACTED] failed to assess the first available security patch within 30 days of availability, and ended on December 22, 2017, when [REDACTED] decommissioned the [REDACTED] switches.

Aggregate Contributing Causes for CIP-007-3a R3 Alleged Violations

552. The primary cause of the CIP-007-3a R3 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] process for assessing patches did not clearly define the individual roles and responsibilities. Additional training, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violations.

Aggregate Risk Assessment for CIP-007-3a R3 Alleged Violations

553. The Regions determined that the CIP-007-3a R3 Alleged Violations posed an aggregate serious or substantial risk¹¹⁰ to the reliability of the Bulk Power System.¹¹¹ The risk posed by [REDACTED] failure to monitor vendor security patches and vulnerability notifications was providing the opportunity for infiltration of unauthorized network traffic into the ESP. However, [REDACTED] maintained the CCAs within a secured ESP inside an established PSP, and [REDACTED]. Despite these protective measures, the aggregate risk remains serious and substantial because in the second Alleged Violation, [REDACTED] failed to monitor for applicable patches and vulnerabilities for the [REDACTED] switches for over 20 months.

Mitigating Actions for CIP-007-3a R3 Alleged Violations

554. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-007-3a R3 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
555. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
556. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED]

¹¹⁰ [REDACTED] individually, posed a moderate risk to the reliability of the BPS, and [REDACTED] individually, posed a serious risk.

¹¹¹ CIP-007-3a R3.1 has a VRF of “Lower” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

completion of the Mitigation Activities and promptly report its successful completion to NERC.

X. CIP-007-6 R3 [REDACTED]

557. 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.

558. CIP-007-6 R3 provides in relevant part:

R3. 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 R3 – Malicious Code Prevention.

P3.1. Deploy method(s) to deter, detect, or prevent malicious code.

....

P3.3. For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.

Description of Alleged Violation and Risk Assessment for [REDACTED]

559. On September 5, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-007-6 R3; P3.3. *See* Self-Report, **Attachment 26a**.

560. On May 12, 2017, during an internal assessment, [REDACTED] discovered that between December 1, 2016 and April 18, 2017, it had tested and installed antivirus signatures for all BES Cyber Assets in one facility but was unable to provide evidence demonstrating the process used to update the signatures.

561. The Alleged Violation affected [REDACTED]
[REDACTED]

562. The primary cause of the CIP-007-6 R3 Alleged Violation was lack of managerial oversight. A contributing cause was inadequate internal controls. There was no work ticketing tool in place for generating CIP compliance tasks; therefore, the compliance analyst could not effectively perform evaluations and store evidence. Proper managerial oversight should have implemented stronger internal controls to help ensure that the process was followed.

563. The Alleged Violation started on December 1, 2016, when [REDACTED] failed to document

its performance of the tested and installed signatures, and ended on April 19, 2017, when [REDACTED] began documenting its performance of the tested and installed signatures.

564. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the Bulk Power System.¹¹² [REDACTED] failure to document the testing and installation of antivirus signatures, could cause missing updates, which could compromise BES Cyber Assets. The risk was mitigated because the signatures were tested and installed. Additionally, the affected system had no external Internet connectivity, and accessing the system required login credentials. Moreover, the system and associated Cyber Assets were inside both an ESP and PSP and were monitoring and logging for Cyber Security Incidents, physical intrusion, and loss of functionality.

Mitigating Actions for CIP-007-6 R3 Alleged Violations

565. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-007-6 R3 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
566. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
567. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED]

¹¹² CIP-007-6 P3.3 has a VRF of “Medium” pursuant to CIP-007-6 Table of Compliance Elements. According to the VSL Matrix, this issue warranted a “Moderate” VSL.

completion of the Mitigation Activities and promptly report its successful completion to NERC.

Y. CIP-007-6 R4

568. CIP-007 ensures that Responsible Entities define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter.

569. CIP-007-6 R4 provides:

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.

P4.1. 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.

4.1.4. 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.

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.

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.

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 Alleged Violation for



2017, [REDACTED] determined that it had not identified [REDACTED] servers as EACMSs. As result, the EACMSs did not generate alerts for security events (P4.2), and [REDACTED] did not review logged events for cyber security events at least every 15 calendar days (P4.4).

576. This instance affected [REDACTED]
[REDACTED]

577. In the fourth instance, during a categorization meeting on August 1, 2017, [REDACTED] discovered that it had not identified one device as a PCA. As a result, [REDACTED] failed to implement security event logging for the PCA as required by CIP-007-6 R4; P4.1 – P4.4.

578. This instance affected [REDACTED]
[REDACTED]

579. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED], the date [REDACTED] committed to complete its Mitigation Plan.

Description of Alleged Violation for [REDACTED]

580. During a Compliance Audit conducted [REDACTED]
[REDACTED], the Regions determined that [REDACTED] as a [REDACTED] [REDACTED] [REDACTED] and [REDACTED] was in violation of CIP-007-6 R4; P4.4. *See PV Summary, Attachment 27e.*

581. Between July 1, 2016 and August 2, 2016, [REDACTED] did not review a summarization or sampling of logged events at least every 15 calendar days to identify undetected Cyber Security Incidents.

582. The Alleged Violation affected approximately [REDACTED]
[REDACTED]

583. The Alleged Violation started on July 16, 2016, the day [REDACTED] was required to conduct a review of logged events, and ended on August 2, 2016, when [REDACTED] conducted a review of the logged events.

Aggregate Root Cause for CIP-007-6 R4 Alleged Violations

584. The primary cause of the CIP-07-6 R4 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process to help ensure that the process was sufficient and followed. Regarding the first Alleged Violation where [REDACTED] failed to identify EACMSs and PACSs, [REDACTED] personnel lacked adequate training to

identify in-scope EACMSs and PACSs. Regarding the second Alleged Violation where █████ failed to review logged events, █████ process did not clearly define the individual roles and responsibilities for implementing security event logging. In addition, the process did not require and there was no internal control to verify the implementation of █████ settings. Additional training, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violation.

Aggregate Risk for CIP-007-6 R4 Alleged Violations

585. The Regions determined that the CIP-007-6 R4 Alleged Violations posed an aggregate serious or substantial risk¹¹⁶ to the reliability of the Bulk Power System.¹¹⁷ The risk posed by █████ failure to implement event monitoring was the unauthorized access to Critical Cyber Assets without █████ knowledge. However, for first instance of the first Alleged Violation, █████ were protected by a whitelisting application to deter malicious code. Additionally, none of the █████ were remotely accessible from outside the PSPs.
586. Notwithstanding, the aggregate was serious and substantial because security event logging for the █████ did not occur for the █████ for over 13 months, which substantially increased the risk of compromise to █████ systems. Additionally, although the unidentified EACMSs were logging, for over two years, the EACMSs did not generate alerts for security events, and █████ did not review logged events for cyber security events. Moreover, for over two years, no security event logging for the PCA had been implemented.

Mitigating Actions for CIP-007-6 R4 Alleged Violations

587. On September 11, 2018, █████ submitted to █████ its final Mitigation Activities to address the CIP-007-6 R4 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, █████ accepted the Mitigation Activities.
588. In the Mitigation Activities, █████ committed to take the following actions by █████ (i) revise its overarching corporate █████ program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each █████ business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the █████ program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures,

¹¹⁶ █████, individually, posed a serious and substantial risk to the reliability of the BPS, and █████, individually, posed a moderate risk.

¹¹⁷ CIP-007-6 P4.1 has a VRF of “Medium” pursuant to CIP-007-6 Table of Compliance Elements. According to the VSL Matrix, this issue warranted a “Severe” VSL.

including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

589. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

Z. CIP-007-3a R5 [REDACTED]
[REDACTED]

590. CIP-007 ensures that Responsible Entities define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter.

591. CIP-007-3a R5 provides:

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimizes the risk of unauthorized system access.

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

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.

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

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with



Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

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

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.



Description of Alleged Violation for [REDACTED]

592. On August 29, 2016, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-007-3a R5.1. *See* Self-Report, **Attachment 28a**. This Alleged Violation involved the sharing of an authorized individual's user account with two unauthorized individuals.
593. On August 28, 2013, [REDACTED] removed system shared user accounts, and implemented individual user accounts, on devices inside a [REDACTED], which service technicians utilized to access and perform maintenance. On May 9, 2016, a [REDACTED] maintenance manager reported that a [REDACTED] service technician was sharing his username and password to access devices inside the [REDACTED] with two team-member service technicians who did not have authorized electronic access to the devices. Although these two service technicians required access to perform their duties, due to an oversight, [REDACTED] did not authorize or grant them individual authorized access after the device upgrade in August 2013. The unauthorized access involved Critical Cyber Assets (CCAs) at one [REDACTED] that housed [REDACTED] Cyber Assets (CAs).
594. On May 9, 2016, the technician who had been sharing his username and password informed his manager about the shared account information. On May 12, 2016, the manager instructed the employees to stop sharing account information and for the authorized employee to change his account password.
595. The Alleged Violation started on August 28, 2013, when the two service technicians gained unauthorized access to CAs inside the [REDACTED] by utilizing the authorized technician's individual user account credentials, and ended on May 12, 2016, when the authorized employee changed his individual user account password.

Description of Alleged Violation for [REDACTED]

596. On January 18, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] and [REDACTED] they were in violation of CIP-007-3a R5.2.¹¹⁸ *See* Self-Report, **Attachment 28b**. [REDACTED] did not identify and inventory an application account deployed on [REDACTED] electronic access control and monitoring systems (EACMSs).
597. On [REDACTED], while preparing for an upcoming Compliance Audit, [REDACTED] discovered that it failed to document an application account deployed on [REDACTED] EACMSs in [REDACTED] control centers that housed high impact BES Cyber Systems. On December 9, 2014, [REDACTED] upgraded its EACMSs with a system shared user account.

¹¹⁸ The Alleged Violation was self-reported under CIP-007-6 R5; P5.2; however, the Regions determined that CIP-007-3a is the applicable Standard because of the start date of the noncompliance.

Because the account is non-interactive/non-user, the account did not show up on the user access or identity management activity reports. On June 23, 2016, [REDACTED] reassigned the compliance responsibility for the EACMSs from the [REDACTED] [REDACTED] group to the [REDACTED]. The [REDACTED] [REDACTED] created system baselines, but the account did not show up on the baselines because it was a non-interactive/non-user account.

598. The Alleged Violation started on December 9, 2014, when [REDACTED] created the system shared account, and ended on November 18, 2016, when [REDACTED] identified and began managing the scope and acceptable use of the system shared user account.

Description of Alleged Violation for [REDACTED]

599. On September 22, 2015, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-007-3a R5.3.3. *See* Self-Report, **Attachment 28c**. [REDACTED] failed to timely reset passwords on authorized electronic access accounts for a CCA.
600. On April 29, 2015, while in the field performing routine maintenance, [REDACTED] discovered that the “read-only” passwords on a single [REDACTED] within one of its [REDACTED] [REDACTED] remained unchanged after the expiration of the mandatory annual password change deadline on December 31, 2014. According to [REDACTED] the firmware on the [REDACTED] did not properly execute the save function when the password change occurred. [REDACTED] provided the 2013 password change ticket demonstrating that on December 18, 2013, it had successfully changed the [REDACTED] passwords. [REDACTED] also provided a 2015 password change ticket as evidence of the current successful password change dated June 29, 2015.
601. The Alleged Violation started on January 1, 2015, when [REDACTED] was required to have changed the [REDACTED] passwords, and ended on June 29, 2015, when [REDACTED] changed the passwords.

Description of Alleged Violation for [REDACTED]

602. On September 5, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-007-3a R5.2 and R5.3. *See* Self-Report, **Attachment 28d**. [REDACTED] failed to timely change passwords on multiple BES Cyber Assets (BCAs).
603. In December 2016, [REDACTED] performed annual password changes for all BCAs. On February 20, 2017, while analyzing a quality assurance review of password changes, [REDACTED] discovered [REDACTED] instances where it had not changed factory default passwords for remotely accessible BCAs as required by CIP-007-3a R5.2. Because the default passwords were never changed, [REDACTED] was also in violation of CIP-007-3a R5.3 for not changing the passwords at least annually.

[REDACTED]

account deployed on [REDACTED] EACMSs, the account was non-interactive and required physical access to the system to make changes. The account password was randomly generated and unknown to the system users. The account was an application system account used for back-end communication between system processes, and according to vendor documentation and [REDACTED] was unable to remove, disable, or rename the account.

608. Notwithstanding, the aggregate risk remains serious and substantial because in the fourth Alleged Violation, [REDACTED] failed to change [REDACTED] default passwords on multiple CAs, and [REDACTED] did not have a quality assurance process for remotely accessible BCAs. Additionally, the Alleged Violation affected [REDACTED], [REDACTED], [REDACTED], and the duration was over six years.

Mitigating Actions for CIP-007-3a R5 Alleged Violations

609. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-007-3a R5 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
610. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
611. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

AA. CIP-007-6 R5

612. CIP-007 ensures that Responsible Entities define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter.

613. CIP-007-6 R5 provides:

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.

P5.1. Have a method(s) to enforce authentication of interactive user access, where technically feasible.

P5.2. Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).

P5.3. Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).

P5.4. Change known default passwords, per Cyber Asset capability.

P5.5. 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, nonalphanumeric) or the maximum complexity supported by the Cyber Asset.

P5.6. Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.

P5.7. Where technically feasible, either:

- Limit the number of unsuccessful authentication attempts; or
- Generate alerts after a threshold of unsuccessful authentication attempts.



Description of Alleged Violation for [REDACTED]

614. On July 19, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED], [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] [REDACTED] and [REDACTED] they were in violation of CIP-007-6 R5; P5.7. *See* Self-Report, **Attachment 29a**. On April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation CIP-007-6 R5; P5.2; P5.3; and P5.7.¹²¹ *See* Self-Report, **Attachment 29b**. On January 23, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation CIP-007-6 R5; P5.2; P5.3; and P5.7.¹²² *See* Self-Report, **Attachment 29c**. On November 27, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-007-6 R5; P5.7.¹²³ *See* Self-Report, **Attachment 29d**. This Alleged Violation involved four instances were [REDACTED] failed to implement system access controls to Cyber Assets (CAs) within Electronic Security Perimeters (ESPs) in accordance with CIP-007-6 R5.
615. In the first instance, [REDACTED] did not document technical limitations of CAs or request a Technical Feasibility Exception (TFE). Specifically, on May 3, 2017, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
616. In the second instance, during a CA categorization review on January 5, 2017, [REDACTED] discovered that [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
617. This instance affected [REDACTED] [REDACTED] [REDACTED] [REDACTED]
618. In the third instance, as part of an extent of condition assessment on November 15,

¹²¹ This noncompliance was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-007-6 R5 is the applicable Standard and Requirement.

¹²² This noncompliance was self-reported as CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-007-6 R5 is the applicable Standard and Requirement.

¹²³ This noncompliance was self-reported as CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to PACS; therefore, the Regions determined that CIP-007-6 R5 is the applicable Standard and Requirement.



2017, [REDACTED] determined that [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

619. This instance affected a total of [REDACTED]
[REDACTED]

620. In the fourth instance, during a categorization meeting on August 1, 2017, [REDACTED] discovered that it had not identified one device as a PCA. As a result, [REDACTED] failed to implement system access controls on the PCA as required by CIP-007-6 R5; P5.1 – P5.7.

621. This instance affected [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED]

622. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED], the date [REDACTED] committed to complete its Mitigation Plan.

Description of Alleged Violation for [REDACTED]

623. On November 28, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] stating that, as a [REDACTED] [REDACTED] was in violation of CIP-007-6 R5; P5.2. *See* Self-Report, **Attachment 29e**.

624. On July 1, 2017, while performing a vulnerability assessment, [REDACTED] discovered [REDACTED]
[REDACTED]
[REDACTED]

625. The Alleged Violation affected [REDACTED] [REDACTED] [REDACTED]
[REDACTED]

626. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED] the date [REDACTED] committed to complete its Mitigation Plan.

Description of Alleged Violation for [REDACTED]

627. On June 19, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-007-6 R5; P5.6. *See* Self-Report, **Attachment 29f**. [REDACTED] failed to timely change passwords to [REDACTED] BCAs.



Aggregate Risk for CIP-007-6 R5 Alleged Violations

632. The Regions determined that the CIP-007-6 R5 Alleged Violations posed an aggregate serious or substantial risk¹²⁴ to the reliability of the Bulk Power System.¹²⁵ The risk posed by [REDACTED] failure to implement system access controls on Cyber Assets within ESPs was providing the opportunity to allow a malicious hacker to gain access to CAs within the ESP through overlooked and unprotected accounts and potentially disrupt operations and cause grid disturbances. However, for all three Alleged Violations, [REDACTED] maintained the all devices within a secured Physical Security Perimeter both with real-time monitoring and alerting enabled. For all Alleged Violations, except for the instances where [REDACTED] failed to identify EACMSs and the PCA, the devices were within a secured ESP. Moreover, the BCAs are isolated from corporate networks.
633. Notwithstanding, the aggregate risk was serious and substantial because in the second Alleged Violation, there were [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] Moreover, for over two years, no system access controls were implemented on the PCA.

Mitigating Actions for CIP-007-6 R5 Alleged Violations

634. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-007-6 R5 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
635. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement

¹²⁴ [REDACTED] individually, posed a serious and substantial risk to the reliability of the BPS, and [REDACTED] individually, posed a moderate risk.

¹²⁵ CIP-007-6 R5 has a VRF of “Medium” pursuant to CIP-007-6 Table of Compliance Elements. According to the VSL Matrix, this issue warranted a “Severe” VSL.

Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

636. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

BB. CIP-007-3a R6 [REDACTED]

637. CIP-007 ensures that Responsible Entities define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter.

638. CIP-007-3a R6 provides in relevant part:

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

Description of Alleged Violation and Risk Assessment for [REDACTED]

639. During a Compliance Audit conducted [REDACTED], the Regions determined that [REDACTED] as a [REDACTED] [REDACTED] and [REDACTED] was in violation of CIP-007-3a R6.2. See PV Summary, **Attachment 30a**. [REDACTED] did not ensure that security-monitoring controls to generate alerts for unsuccessful login thresholds were properly implemented.

640. The Regions discovered that on April 30, 2015, when [REDACTED] implemented a new security information and event management (SIEM) tool, it made configuration errors, which prevented email alerts for detected cyber security incidents, such as unauthorized access attempts to Cyber Assets (CAs) within the Electronic Security Perimeter (ESP), to be generated to response personnel.

641. The primary cause of the CIP-007-3a R6 Alleged Violation was lack of managerial oversight. Contributing causes included a deficient process, inadequate training,

and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] process did not clearly define the individual roles and responsibilities. Additional training on the new cyber security testing software, along with clearer instructions for completing tasks and stronger internal controls could have helped prevent the Alleged Violation.

642. The Alleged Violation started on April 30, 2015, when [REDACTED] misconfigured the SIEM tool, which prevented alerts for unsuccessful login attempts, and ended on November 11, 2015, when [REDACTED] reconfigured the SIEM tool and alerting for unsuccessful login attempts resumed.
643. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the Bulk Power System.¹²⁶ The risk posed was that alerts would not have been issued for detected system security events, which could have allowed an attacker to gain access to systems without [REDACTED] knowledge. The risk was mitigated because [REDACTED] maintained CAs within both a secured ESP and PSP, both with real-time monitoring and alerting enabled. Additionally, access was restricted to authorized personnel who were current on cyber security training and had a valid personnel risk assessment on file.

Mitigating Actions for [REDACTED]

644. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-007-3a R6 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
645. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation

¹²⁶ CIP-007-3a R6.2 has a VRF of “Lower” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.

Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

646. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

CC. CIP-007-3a R7 [REDACTED]

647. CIP-007 ensures that Responsible Entities define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter.

648. CIP-007-3a R7 provides in relevant part:

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

Description of Alleged Violation and Risk Assessment for [REDACTED]

649. On August 11, 2016, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-007-3a R7.1. *See Self-Report, Attachment 31a.* [REDACTED] failed to implement its internal disposal and redeployment program to help prevent unauthorized retrieval of sensitive cyber security or reliability data.

650. On February 18, 2016, a Critical Cyber Asset (CCA) device within a critical asset [REDACTED] Physical Security Perimeter (PSP) failed. On February 24, 2016, [REDACTED] replaced the device and transported it to [REDACTED] sanitizing facility PSP where [REDACTED] sanitized the device. On February 25, 2016, another CCA device failed at another critical asset [REDACTED]. On February 29, 2016, [REDACTED] transported the device to its sanitizing facility PSP and sanitized it on March 1, 2016. In both instances, [REDACTED] failed to implement its internal disposal and redeployment program, which requires the device to remain within the designated PSP until a proper chain of custody process is followed to transport the device in a secured container to the appropriate sanitizing facility.

651. The primary cause was an inadequate process. [REDACTED] process did not clearly define

the roles and responsibilities regarding the chain of custody.

652. The first instance started on February 24, 2016, when the [REDACTED] employee transported the device without properly securing it, and ended on February 24, 2016, when [REDACTED] received the device at the sanitizing location and sanitized it. The second instance started on February 29, 2016, when the [REDACTED] employee transported the device without properly securing it, and ended on February 29, 2016, when [REDACTED] received the device at the sanitizing location and sanitized it.
653. The Regions determined that the Alleged Violation posed a minimal risk to the reliability of the Bulk Power System.¹²⁷ The risk posed was providing the opportunity for exploitation of discarded CCAs that have not been properly sanitized. The risk was mitigated because the devices remained in the possession of [REDACTED] employees during the transportation and sanitization of the devices. The [REDACTED] employees involved with the delivery and sanitization of the devices had authorized electronic and physical access to the devices.

Mitigating Actions for [REDACTED]

654. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-007-3a R7 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
655. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

¹²⁷ CIP-007-3a R7.1 has a VRF of “Lower” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.



656. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

DD. CIP-007-3a R8 [REDACTED]

657. CIP-007 ensures that Responsible Entities define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter.

658. CIP-007-3a R8 provides:

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

- 8.4.** Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

Description of Alleged Violation and Risk Assessment for [REDACTED]

659. On September 2, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED], [REDACTED] was in violation of CIP-007-3a R8.4. *See Self-Report, Attachment 32a.* [REDACTED] did not document a Cyber Vulnerability Assessment (CVA) action plan to remediate or mitigate vulnerabilities.

660. On November 17, 2015, [REDACTED] completed its annual CVA on Cyber Assets (CAs) associated with a [REDACTED] and a [REDACTED]. The team identified vulnerabilities during the CVA, but did not create a formal mitigation action plan to remediate or mitigate identified vulnerabilities. On January 6, 2016, during an internal controls assessment testing, [REDACTED] discovered that the [REDACTED] did not create the required CVA vulnerability action plan. On March 9, 2016, the [REDACTED] documented the action items to mitigate vulnerabilities discovered during the November 17, 2015, CVA. On March 23, 2016, the [REDACTED] performed an additional CVA to confirm that [REDACTED] had addressed the previously identified vulnerabilities, and no new vulnerabilities existed.

661. The primary cause was ineffective training. [REDACTED] process did not clearly define individual roles and responsibilities. The IT support team did not believe the

identified vulnerabilities would be handled in an ongoing patch procedure and by enabling/disabling system logs.

662. The Alleged Violation started on November 17, 2015, when █████ failed to document the CVA vulnerability action plan, and ended on March 9, 2016, when █████ documented the vulnerability action plan
663. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the Bulk Power System.¹²⁸ The risk posed by █████ failure to document a vulnerability action plan was providing the opportunity of unauthorized access and exploitable vulnerabilities to CCAs and/or other CAs located within █████ ESP without █████ knowledge. However, although █████ did not formally document each identified vulnerability action plan, █████ had on-going processes to address each vulnerability through its testing and patching processes. █████ maintained CAs within both a secured ESP and PSP, both with real-time monitoring and alerting enabled.

Mitigating Actions for █████

664. On September 11, 2018, █████ submitted to █████ its final Mitigation Activities to address the CIP-007-3a R8 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, █████ accepted the Mitigation Activities.
665. In the Mitigation Activities, █████ committed to take the following actions by █████
█████ (i) revise its overarching corporate █████ program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each █████ business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the █████ program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) █████ will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

¹²⁸ CIP-007-3a R8.4 has a VRF of “Lower” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “Severe” VSL.



666. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

EE. CIP-007-3a R9 [REDACTED]

667. CIP-007 ensures that Responsible Entities define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter.

668. CIP-007-3a R9 provides:

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

Description of Alleged Violation and Risk Assessment for [REDACTED]

669. On October 17, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-007-3a R9.¹²⁹ See Self-Report, **Attachment 33a.** [REDACTED] failed to document modifications to systems and controls to a Cyber Asset (CA) inside an Electronic Security Perimeter (ESP) within 30 calendar days.
670. On June 8, 2017, during an asset inventory walk-down, [REDACTED] discovered a modem with a working phone line, which was connected to a communications processor located at a medium impact [REDACTED]. The modem had been listed on [REDACTED] asset diagram during the January 7, 2015 initial asset inventory walk-down.
671. On April 6, 2016, [REDACTED] replaced the communications processor with a new one but left the modem in place and attached it to a different Critical Cyber Asset (CCA). Because the modem used a routable protocol, the modem was not necessary and thus should have been removed from the substation but was not until more than a year later. Regardless, [REDACTED] made modifications to systems and controls but failed to document the changes within 30 calendar days from the modifications.
672. As a result, the modem should not have remained on the asset diagram because it was not serving as a CCA, and the system configuration was such that it did not permit electronic communication between the modem and the CCA. On June 11,

¹²⁹ The Alleged Violation was self-reported under CIP-002-5.1 R1.2; however, the Regions determined that CIP-007-3a R9 is the applicable Standard and Requirement.



2017, [REDACTED] removed the modem from the [REDACTED]

673. The primary cause was lack of training. When the design team designed the changes to replace the communications processor, they did not recognize the need to remove the modem.
674. The Alleged Violation began on May 6, 2016, 30 calendar days after [REDACTED] made modifications to systems and controls and did not document the modifications, and ended on June 11, 2017, when [REDACTED] removed the modem from service.
675. The Regions determined that the Alleged Violation posed a minimal risk to the reliability of the Bulk Power System.¹³⁰ The risk posed by [REDACTED] failure to properly configure and document changes to a CCA was providing the opportunity for insufficient protective measures, exposing the CCA to unauthorized or malicious actions. The risk was mitigated because the affected CCA did not have an active port with the modem, rendering dial-up communications with the CCA and malicious actions impossible.

Mitigating Actions for [REDACTED]

676. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-007-3a R9 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
677. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

¹³⁰ CIP-007-3a R9 has a VRF of “Lower” pursuant to the VRF Matrix. According to the VSL Matrix, this issue warranted a “High” VSL.



678. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

FF. CIP-009-6 R1 [REDACTED]

679. CIP-009-6 helps Registered Entities 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.

680. CIP-009-6 R1 provides:

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.

P1.1 Conditions for activation of the recovery plan(s).

P1.2 Roles and responsibilities of responders.

P1.3 One or more processes for the backup and storage of information required to recover BES Cyber System functionality.

P1.4 One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.

P1.5 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 Alleged Violation for [REDACTED]

681. On April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-009-6 R1; P1.1; P1.2; P1.3; P1.4; and P1.5.¹³¹ See Self-Report, **Attachment 34a**. On January 23, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation of CIP-009-6 R1; P1.1; P1.2;

¹³¹ This noncompliance was self-reported as CIP-002-5.1a R1. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-009-6 R1 is the applicable Standard and Requirement.

P1.3; P1.4; and P1.5.¹³² See Self-Report, **Attachment 34b**. This Alleged Violation includes two instances where [REDACTED] failed to include Electronic Access Control Monitoring Systems (EACMSs) in its documented Recovery Plan.

682. In the first instance, during a Cyber Asset (CA) categorization review on January 5, 2017, [REDACTED] discovered that it had not identified [REDACTED] as EACMSs. As a result, [REDACTED] failed to include these EACMSs in its documented Recovery Plan.
683. This instance affected [REDACTED]
[REDACTED] [REDACTED] [REDACTED]
684. In the second instance, as part of an extent of condition assessment on November 15, 2017, [REDACTED] determined that it had not identified [REDACTED] servers as EACMSs. As a result, [REDACTED] failed to include these EACMSs in its documented Recovery Plan.
685. This instance affected a total of [REDACTED] [REDACTED]
[REDACTED]
686. The primary cause of the Alleged Violation was lack of managerial oversight. A contributing cause was inadequate training. [REDACTED] training lacked the specificity to identify all EACMSs. Proper managerial oversight should have identified and prevented training deficiencies to help ensure that the CA identification process was followed. Additional training along with clearer instructions for completing tasks could have helped prevent the Alleged Violation.
687. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on March 31, 2018, when [REDACTED] included the EACMSs in its Recovery Plan.
688. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the Bulk Power System (BPS).¹³³ The risk posed by [REDACTED] failure to include the EACMSs in its Recovery Plan was providing the opportunity that [REDACTED] would be unable to recover from an attack on its systems, which could negatively affect BPS reliability. However, [REDACTED] deployed the devices in question behind a firewall, logged events to detect malicious code, as well as successful and failed login attempts, and changed known default password per Cyber Asset capability and enforced password complexity. [REDACTED] also deployed methods to enforce authentication of interactive user access.

¹³² This noncompliance was self-reported as CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-009-6 R1 is the applicable Standard and Requirement.

¹³³ CIP-009-6 R1 has a VRF of “Medium” pursuant to CIP-007-6 Table of Compliance Elements. According to the VSL Matrix, this issue warranted a “Severe” VSL.

Mitigating Actions for CIP-009-6 R1 Alleged Violations

689. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-009-6 R1 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
690. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
691. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

GG. CIP-009-6 R2 [REDACTED]

692. CIP-009-6 R2 helps Registered Entities 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.
693. CIP-009-6 R2 provides in relevant part:
- R2.** Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.
- P2.1.** Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months:
- By recovering from an actual incident;



- With a paper drill or tabletop exercise; or
- With an operational exercise.

P2.2. Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.

....

Description of Alleged Violation for [REDACTED]

694. On January 23, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation of CIP-009-6 R2; P2.1; and P2.2.¹³⁴ See Self-Report, **Attachment 35a**. On April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-009-6 R2; P2.1, and P2.2.¹³⁵ See Self-Report, **Attachment 35b**. This Alleged Violation includes two instances where [REDACTED] failed to include Electronic Access Control Monitoring Systems (EACMSs) in its implementation and subsequent testing of the documented Recovery Plan.
695. In the first instance, as part of an extent of condition assessment on November 15, 2017, [REDACTED] determined that it had not identified [REDACTED] servers as EACMSs. As a result, [REDACTED] failed to include these EAMCSs in its documented Recovery Plan; thus, the EACMSs were not included in the implementation and subsequent testing of the Recovery Plan.
696. This instance affected [REDACTED] [REDACTED] [REDACTED] [REDACTED]
697. In the second instance, during a Cyber Asset (CA) categorization review on January 5, 2017, [REDACTED] discovered that it had not identified [REDACTED] [REDACTED] as EACMSs. As a result, [REDACTED] failed to include these EACMSs, in its documented Recovery Plan; thus, the EACMSs were not included in the implementation and subsequent testing of the Recovery Plan.

¹³⁴ This noncompliance was self-reported as CIP-002-5.1a R1. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-009-6 R2 is the applicable Standard and Requirement.

¹³⁵ This noncompliance was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-009-6 R2 is the applicable Standard and Requirement.

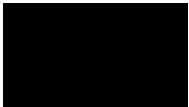


698. This instance affected [REDACTED]
699. The primary cause of the Alleged Violation was lack of managerial oversight. A contributing cause was inadequate training. [REDACTED] training lacked the specificity to identify all EACMSs. Proper managerial oversight should have identified and prevented training deficiencies to help ensure that the CA identification process was followed. Additional training along with clearer instructions for completing tasks could have helped prevent the Alleged Violation.
700. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on March 31, 2018, when [REDACTED] included the EACMSs in the implementation and testing of its Recovery Plan.
701. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the Bulk Power System (BPS).¹³⁶ The risk posed by [REDACTED] failure to include the EACMSs in the implementation and testing of its Recovery Plans was providing the opportunity that [REDACTED] would be unable to recover from an attack on its systems, which could negatively affect BPS reliability. However, [REDACTED] deployed the devices in question behind a firewall, logged events to detect malicious code, as well as successful and failed login attempts, and changed known default passwords per Cyber Asset capability and enforced password complexity. [REDACTED] also deployed methods to enforce authentication of interactive user access.

Mitigating Actions for CIP-009-6 R2 Alleged Violations

702. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-009-6 R2 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
703. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard

¹³⁶ CIP-009-6 R2 has a VRF of “Lower” pursuant to CIP-007-6 Table of Compliance Elements. According to the VSL Matrix, this issue warranted a “Severe” VSL.



and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

704. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

HH. CIP-009-6 R3 [REDACTED]

705. CIP-009-6 helps Registered Entities 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.

706. CIP-009-6 R3 provides:

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.

P3.1. No later than 90 calendar days after completion of a recovery plan test or actual recovery:

P3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.

P3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and

P3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.

P3.2. No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the

- [REDACTED]
- [REDACTED]
712. In the third instance, as part of an extent of condition assessment on November 15, 2017, [REDACTED] determined that it had not identified [REDACTED] as EACMSs. As a result, [REDACTED] failed to include these EAMCS in its documented Recovery Plan; thus, these EACMSs were not included in the reviews and updates of [REDACTED] Recovery Plan.
713. This instance affected [REDACTED]
714. The primary cause of the CIP-009-6 R3 Alleged Violation was lack of managerial oversight. A contributing cause was inadequate training. [REDACTED] training lacked the specificity to identify all EACMSs. Proper managerial oversight should have identified and prevented training deficiencies to help ensure that the CA identification process was followed. Additional training along with clearer instructions for completing tasks could have helped prevent the Alleged Violation.
715. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on March 31, 2018, when [REDACTED] included these EACMSs in the review and update of its Recovery Plan.
716. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the Bulk Power System (BPS).¹⁴⁰ [REDACTED] failure to develop and maintain a recovery plan for these EACMSs could leave [REDACTED] unable to recover from an attack which could negatively affect BPS reliability. However, [REDACTED] deployed the devices in question behind a firewall, it logged events to detect malicious code, as well as successful and failed login attempts, and it changed known default password per Cyber Asset capability and enforced password complexity. [REDACTED] also deployed methods to enforce authentication of interactive user access.

Mitigating Actions for CIP-009-6 R3 Alleged Violations

717. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-009-6 R3 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
718. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal

¹⁴⁰ CIP-009-6 R3 has a VRF of “Lower” pursuant to CIP-007-6 Table of Compliance Elements. According to the VSL Matrix, this issue warranted a “Severe” VSL.

[REDACTED]

controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

719. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

II. CIP-010-2 R1 [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

720. CIP-010-2 prevents and detects 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 Bulk Electric System (BES).

721. CIP-010-2 R1 provides:

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.

P1.1. Develop a baseline configuration, individually or by group, which shall include the following items:

P1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;

P1.1.2. Any commercially available or open-source application software (including version) intentionally installed;

P1.1.3. Any custom software installed;



P1.1.4. Any logical network accessible ports; and

P1.1.5. Any security patches applied.

P1.2. Authorize and document changes that deviate from the existing baseline configuration.

P1.3. For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

P1.4 For a change that deviates from the existing baseline configuration:

P1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;

P1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected.

....

Description of Alleged Violation for [REDACTED]

722. During a Compliance Audit conducted [REDACTED], the Regions determined that [REDACTED] as [REDACTED] was in violation of CIP-010-2 R1; P1.1.¹⁴¹ See PV Audit Summary, **Attachment 37a**. [REDACTED] failed to maintain an accurate baseline configuration because it included devices on its baseline that were no longer part of the BES Cyber System.
723. From a sampled BCA inventory list, the Regions performed a walk-down of a [REDACTED] and discovered [REDACTED] BCAs that had been identified on the BCA inventory list could not be located within the [REDACTED]. The [REDACTED] BCAs were decommissioned on December 23, 2015, but [REDACTED] failed to update the BCA inventory list.
724. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED] the date [REDACTED] committed to complete its Mitigation Plan.

Description of Alleged Violation for [REDACTED]

725. On August 9, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED], [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] and [REDACTED] they were in violation of

¹⁴¹ The Alleged Violation was identified under CIP-002-5.1 R1.2; however, the Regions determined that CIP-010-2 R2; P1.1 is the applicable Standard and Requirement.

[REDACTED]

CIP-010-2 R1; P1.1.1. *See* Self-Report, **Attachment 37b**. [REDACTED] failed to develop accurate baseline configurations.

726. On June 14, 2017, during a Cyber Vulnerability Assessment (CVA) review, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
727. The Alleged Violation affected [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]
728. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on June 21, 2017, when [REDACTED] updated the baseline configurations to reflect the firmware version installed on the [REDACTED].

Description of Alleged Violation for [REDACTED]

729. On November 28, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED], [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED] they were in violation of CIP-010-2 R1; P1.1, P1.1.1, and P1.1.4. *See* Self-Report, **Attachment 37c**. [REDACTED] failed to develop accurate baseline configurations.
730. On July 1, 2017, during [REDACTED] first annual CVA associated to CIP-010-2 R1, it discovered that it had failed to include [REDACTED] BCAs in its baseline configurations. Additionally, [REDACTED] failed to include [REDACTED] BCAs and [REDACTED] PCAs on the correct baseline configurations. For [REDACTED] BCAs, [REDACTED] installed the firmware version that was authorized, but it made administrative errors when creating the baseline configurations (P1.1.1). Moreover, [REDACTED] incorrectly documented in its baseline configurations one port associated with [REDACTED] BCAs used by administrators as a backup to analyze events (P1.1.4). All BCAs and PCAs in these instances were associated to Medium Impact BCSs.
731. The Alleged Violation started on July 1, 2016, when Standard became mandatory and enforceable, and will end on [REDACTED] when [REDACTED] committed completed its Mitigation Plan.

Description of Alleged Violation for [REDACTED]

732. On September 2, 2016, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-010-2 R1; P1.1.4. *See* Self-Report, **Attachment 37d**. [REDACTED] failed to include enabled logical network ports in its baseline configuration for five Cyber Asset (CA) devices located at two different facilities.



733. On August 1, 2016, the [REDACTED] team conducted an audit readiness workshop and discovered five devices with baseline documentation that did not match the device configurations. [REDACTED] identified [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

734. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on September 2, 2016, when [REDACTED] updated its baselines.

Description of Alleged Violation for [REDACTED]

735. During a Compliance Audit conducted [REDACTED], the Regions determined that [REDACTED] as a [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED] was in violation of CIP-010-2 R1; P1.1.4. See PV Audit Summary, **Attachment 37e**. [REDACTED] failed to include enabled logical network accessible ports in its baseline configuration for one EACMS.

736. In December 2014, [REDACTED] deployed the EACMS but did not perform a network port scan to confirm that it had documented all logical network accessible ports. Following an audit team data request, [REDACTED] determined that two ports had been open since the implementation of the device. On September 16, 2016, [REDACTED] transferred the responsibility for the EACMS to a different team, and the new team performed the required network port scan. On October 28, 2016, [REDACTED] updated the baseline configuration to reflect the enabled logical network accessible ports.

737. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on October 28, 2016, the date [REDACTED] updated the baseline configuration to reflect the enabled logical network accessible ports.

Description of Alleged Violation for [REDACTED]

738. On October 9, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-010-2 R1; P1.1.4.¹⁴² See Self-Report, **Attachment 37f**. [REDACTED] failed to include enabled logical network accessible ports in its baseline configuration.

739. On June 28, 2017, during a review of [REDACTED] and a CVA for a [REDACTED], [REDACTED] discovered that it failed to document in its baseline configuration the enabled logical network accessible ports associated with a server

¹⁴² The Alleged Violation was self-reported under CIP-007-3a R2.1; however, the Regions determined that CIP-010-2 R1; P1.1.4 is the applicable Standard and Requirement.

used to run [REDACTED] software. [REDACTED] procedure for documenting baseline configurations required the use of a port scan. On May 17, 2017, [REDACTED] documented the baseline configuration but the machine used for the port scan ran an older version of the operating system, which did not employ the enabled logical network accessible ports. [REDACTED] procedure for documenting the baseline configuration should have called for specifying the port range per the vendor manual rather than using only a port scan.

740. The Alleged Violation affected [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
741. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on August 18, 2017, the date [REDACTED] updated the baseline to include the missing ports.

Description of Alleged Violation for [REDACTED]

742. On March 29, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-010-2 R1; P1.1.5.¹⁴³ See Self-Report, **Attachment 37g**. [REDACTED] failed to include two security patches in its baseline configuration.
743. On July 26, 2016, [REDACTED] discovered that on June 21, 2016, [REDACTED] applied two patches as an upgrade to an [REDACTED] associated with [REDACTED] BCAs but failed to update the baseline configuration to reflect the changes prior to the effective date of the Standard and Requirement, when [REDACTED] was required to have a current baseline configuration.
744. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on July 26, 2016, the date [REDACTED] updated the baseline configuration.

Description of Alleged Violation for [REDACTED]

745. On February 2, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and a [REDACTED] it was in violation of CIP-010-2 R1; P1.2. See PV Audit Summary, **Attachment 37h**. [REDACTED] did not authorize and document changes that deviated from the existing baseline configuration.
746. On September 1, 2016, during a daily review of software changes, [REDACTED] discovered that on August 31, 2016, it installed configuration management software on [REDACTED] BCAs at a [REDACTED] center without prior authorization and documenting the

¹⁴³ The Alleged Violation was self-reported under R1; P1.3; however, the Regions determined that R1; P1.1 is the applicable Standard Requirement.



changes to the existing baseline configuration.

747. The Alleged Violation started on August 31, 2016, when [REDACTED] implemented unapproved changes to the existing baseline configuration, and ended on September 20, 2016, the date [REDACTED] completed the security controls testing.

Description of Alleged Violation for [REDACTED]

748. On March 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-010-2 R1; P1.2. See Self-Report, **Attachment 37i**. [REDACTED] did not authorize and document changes that deviated from the existing baseline configuration.

749. On February 3, 2017, during a daily routine review of changes to BCAs, [REDACTED] discovered that on February 2, 2017, it implemented two patches to two EACMSs, without prior authorization and documenting the changes to the existing baseline configuration.

750. The Alleged Violation affected [REDACTED] [REDACTED] [REDACTED] [REDACTED]

751. The Alleged Violation started on February 2, 2017, when [REDACTED] implemented the unapproved changes, and ended on February 20, 2017, the date [REDACTED] completed the security controls testing.

Description of Alleged Violation for [REDACTED]

752. On January 12, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] was in violation of CIP-010-2 R1; P1.2. See Self-Report, **Attachment 37j**. [REDACTED] did not authorize and document changes that deviated from the existing baseline configuration.

753. On October 30, 2017, during a daily review of configuration changes, an employee observed that on October 27, 2017, an engineer had installed software on [REDACTED] workstations located at a [REDACTED] without prior authorization. There were two change tickets to install the same software to a total of [REDACTED] workstations, [REDACTED] to be installed on October 27, 2017, and [REDACTED] to be installed on October 31, 2017. However, the engineer who installed the software was not aware that the workstations were split on two change tickets with different installation dates and installed the software to all [REDACTED] workstations at the same time.

754. The Alleged Violation affected [REDACTED] [REDACTED] [REDACTED] [REDACTED]

755. The Alleged Violation started on October 27, 2017, when [REDACTED] implemented the

changes that deviated from the existing baseline without prior authorization, and ended on October 31, 2017, the date [REDACTED] authorized the request to make changes.

Description of Alleged Violation for [REDACTED]

756. During a Compliance Audit conducted [REDACTED], the Regions determined that [REDACTED] as a [REDACTED] [REDACTED] [REDACTED] and [REDACTED] was in violation of CIP-010-2 R1; P1.4.1 and P1.4.2. See PV Audit Summary, **Attachment 37k**. [REDACTED] performed a system upgrade and did not document the cyber security controls impacted by the change, verify the required cyber security controls were not impacted, or document the results of the verification.
757. On [REDACTED], while preparing evidence for an upcoming Compliance Audit, [REDACTED] discovered that on August 31, 2016, it implemented changes to a communications processor, a PCA, which deviated from the existing baseline configuration, without first determining the required security controls in CIP-005 and CIP-007 that could be impacted by the changes per CIP-010-2 P1.4.1. Additionally, following the changes to the PCA, [REDACTED] did not verify that such cyber security controls were not adversely affected per CIP-010-2 P1.4.2.
758. The Alleged Violation started on August 31, 2016, when [REDACTED] failed to identify cyber security controls that could be impacted before implementing changes to existing baseline configurations, and will end on [REDACTED] the date [REDACTED] committed to complete its Mitigation Plan.

Description of Alleged Violation for [REDACTED]

759. On December 18, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-010-2 R1; P1.4.1 and P1.4.2. See Self-Report, **Attachment 37l**. On August 31, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation of CIP-010-2 R1; P1.1; P1.2; and P1.3.¹⁴⁴ See Self-Report, **Attachment 37m**. On April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-010-2 R1; P1.1, P1.2, P1.3, and P1.4.¹⁴⁵ See Self-Report, **Attachment 37n**. On January 23, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation of CIP-010-2

¹⁴⁴ This noncompliance was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-010-2 R1 is the applicable Standard and Requirement.

¹⁴⁵ This noncompliance was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-010-2 R1 is the applicable Standard and Requirement.



R1; P1.1, P1.2, P1.3, and P1.4.¹⁴⁶ See Self-Report, **Attachment 37o**. On November 27, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-010-2 R1; P1.1, P1.2, P1.3, and P1.4.¹⁴⁷ See Self-Report, **Attachment 37p**. This Alleged Violation involves five instances where [REDACTED] failed to fully implement its configuration change management program.

760. In the first instance, [REDACTED] did not identify cyber security controls that could be impacted before implementing changes to existing baseline configurations (P1.4.1) or verify that such controls were not adversely affected after implementing the changes (P1.4.2). Specifically, on September 12, 2017, during reviews of change management testing scans and subsequent review of [REDACTED] internal relevant BES file folders, [REDACTED] discovered that since July 12, 2017, prior to implementing changes to [REDACTED] IDS/IPS systems that deviate from the existing baseline configuration, it did not determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the changes per P1.4.1.
761. Additionally, following the changes to the IDS/IPS systems, [REDACTED] did not verify that such cyber security controls were not adversely affected per P1.4.2. [REDACTED] determined that the [REDACTED] devices were listed on the change ticket to be included in the security controls test, but the devices were not tested. On October 13, 2017, [REDACTED] completed the security controls test for the [REDACTED] devices and documented its verification that the changes in the baseline configuration did not adversely affect cyber security controls in CIP-005 and CIP-007.
762. This instance affected [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
763. In the second instance, on July 20, 2016, during a quarterly CA list review, [REDACTED] discovered that it had not documented [REDACTED] EACM devices (security information and event management Cyber Assets), each protecting a [REDACTED]. Because [REDACTED] failed to identify the EACMSs, it failed to include the devices in its configuration change management program.

¹⁴⁶ This noncompliance was self-reported as CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-010-2 R1 is the applicable Standard and Requirement.

¹⁴⁷ This noncompliance was self-reported as CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to PCAs; therefore, the Regions determined that CIP-010-2 R1 is the applicable Standard and Requirement.



764. This instance affected [REDACTED]
[REDACTED]
765. In the third instance, during a CA categorization review on January 5, 2017, [REDACTED] discovered [REDACTED] operating as EACMSs but not identified as such. As a result, [REDACTED] failed to include these EACMS in its configuration change management program as required by CIP-010-2 R1.
766. This instance affected [REDACTED]
767. In the fourth instance, as part of an extent of condition assessment on November 15, 2017, [REDACTED] determined that it had not identified [REDACTED] servers as EACMSs. As a result, [REDACTED] failed to include these EACMSs in its configuration change management program as required by CIP-010-2 R1.
768. This instance affected [REDACTED]
[REDACTED]
769. In the fifth instance, during a categorization meeting on August 1, 2017, [REDACTED] discovered that it had not identified one device as a PCA. As a result, [REDACTED] failed to include the PCA in its configuration change management program as required by CIP-010-2 R1.
770. This instance affected [REDACTED]
[REDACTED]
771. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED] the date [REDACTED] committed to complete its Mitigation Plan.

Aggregate Contributing Causes of CIP-010-2 R1 Alleged Violations

772. The primary cause of the CIP-010-2 R1 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] configuration change management process did not clearly define the roles and responsibilities of [REDACTED] personnel. For instance, there was confusion as to who was ultimately responsible for approving and documenting changes, which created inconsistent application of the process. Additional training, along with clearer instructions for completing tasks, could have helped prevent the Alleged Violations. Additionally, there was a lack of internal controls to ensure that specific actions required by the process were followed. For example, change requests and

approvals were not always present and/or documented prior to implementing changes.

Aggregate Risk Statement for CIP-010-2 R1 Alleged Violations

773. The Regions determined that the Alleged Violations posed an aggregate serious risk¹⁴⁸ to the reliability of the Bulk Power System based on the following factors.¹⁴⁹ [REDACTED] failure to accurately document and track changes that deviate from existing baseline configurations increased the risk that [REDACTED] would not identify unauthorized changes, which could adversely impact BCSs. Several factors increased the aggregate risk. In the third Alleged Violation, [REDACTED] failed to include seven BCAs in its baseline configurations, while also failing to include [REDACTED] BCAs and [REDACTED] PCAs on the correct baseline. The Regions determined that [REDACTED] had serious, systemic security and compliance issues across its [REDACTED] functional groups, which required [REDACTED] to overhaul its entire CIP compliance program. Because of this, the risk for continued noncompliance and compromise to BCSs and CAs dramatically increased. Due to the weaknesses in [REDACTED] CIP compliance program, the Regions anticipate that [REDACTED] will identify additional instances of noncompliance while completing mitigation, which [REDACTED] will report to the Regions. Notwithstanding, [REDACTED] comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that [REDACTED] reports.

Mitigating Actions for CIP-010-2 R1 Alleged Violations

774. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-010-2 R1 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
775. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a

¹⁴⁸ Alleged Violation [REDACTED] individually posed a serious risk to the reliability of the BPS, [REDACTED], individually, posed a moderate risk, and [REDACTED] [REDACTED] individually, posed a minimal risk.

¹⁴⁹ CIP-010-2 P1 has a VRF of “Medium” pursuant to CIP-010-2 Table of Compliance Elements. According to the VSL Matrix, these Alleged Violations warrant a “Severe” VSL.

mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

776. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

JJ. CIP-010-2 R2 [REDACTED]
[REDACTED]

777. CIP-010-2 R2 provides:

R2. 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 R2 – Configuration Monitoring.

P2.1. Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.

Description of Alleged Violation for [REDACTED]

778. On [REDACTED], during a Compliance Audit conducted [REDACTED], the Regions determined that [REDACTED] and [REDACTED] as [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED] were in violation of CIP-010-2 R2; P2.1. See PV Audit Summary, **Attachment 38a**. This Alleged Violation involves two instances where [REDACTED] failed to monitor for changes to the baseline configurations at least once every 35-calendar days.

779. In the first instance, on [REDACTED], while collecting evidence for upcoming compliance audit, [REDACTED] discovered that it failed to monitor for changes to the baseline configurations for [REDACTED] Electronic Access Control and Monitoring Systems (EACMSs) at least once every 35-calendar days. The next 35-day baseline configuration review was due and scheduled for August 26, 2016, but [REDACTED] did not perform the review until September 8, 2016.

780. This instance affected [REDACTED] [REDACTED] [REDACTED]
[REDACTED]



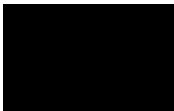
781. This instance started on August 6, 2016, when [REDACTED] was required to monitor for changes to the baseline configurations for the EACMSs, and ended on September 8, 2016, when [REDACTED] monitored for changes to the baseline configurations.
782. In the second instance, during the compliance audit, from a sampling of EACMS devices, the Regions discovered that [REDACTED] failed to monitor for changes to baseline configurations for one EACMS firewall at least once every 35 calendar days.
783. On June 28, 2016, [REDACTED] deployed a new [REDACTED] and the [REDACTED] was unaware that the system was active. Upon activation of the new [REDACTED], the front-end servers were utilizing the communication path through the firewalls to communicate with other BCAs, in effect making the firewall an electronic access point to the ESP. The firewall was active on July 8, 2016, but [REDACTED] did not perform the 35-day baseline configuration review until September 8, 2016.
784. This instance affected [REDACTED]
785. The Alleged Violation started on August 6, 2016, when [REDACTED] was required to monitor for changes to the baseline configurations for the EACMS firewall, and ended on September 8, 2016, when [REDACTED] monitored for changes to the baseline configurations.

Description of Alleged Violation for [REDACTED]

786. On March 29, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-010-2 R2; P2.1. *See* Self-Report, **Attachment 38b**. [REDACTED] did not monitor for changes to the baseline configurations for one firewall at least once every 35-calendar days.
787. On February 13, 2017, while performing a 35-day review for unauthorized changes to the baseline configuration, [REDACTED] discovered a firewall in an [REDACTED] that had not been monitored for changes to the baseline configuration since December 2016. This Alleged Violation affected [REDACTED] BCAs, [REDACTED] EACMS, and [REDACTED] Physical Access Control Systems.
788. The Alleged Violation started on August 5, 2016, when [REDACTED] was required to monitor for changes to the baseline configurations for the firewall, and ended on February 13, 2017, when [REDACTED] monitored for changes to the baseline configuration for the firewall.

Description of Alleged Violation for [REDACTED]

789. On [REDACTED], [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-



795. On May 26, 2017, [REDACTED] completed the last successful scan for changes to the baseline configuration. The next scan for changes would have been due no more than 35 days later by June 30, 2017. On September 29, 2017, monitoring for changes to the baseline configuration for the two IDS/IPS devices resumed.
796. This instance affected [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
797. In the second instance, during a CA categorization review on January 5, 2017, [REDACTED] determined that it had not identified [REDACTED] as EACMSs. As a result, [REDACTED] failed to monitor at least once every 35 calendar days for changes to the EAMCSs baseline configurations and document and investigate detected unauthorized changes.
798. This instance affected [REDACTED]
799. In the third instance, as part of an extent of condition assessment on November 15, 2017, [REDACTED] determined that it had not identified [REDACTED] servers as EACMSs. As a result, [REDACTED] failed to monitor at least once every 35 calendar days for changes to the EACMSs baseline configurations and document and investigate detected unauthorized changes.
800. This instance affected [REDACTED]
[REDACTED]
801. The Alleged Violation started September 4, 2016, when [REDACTED] should have monitored for changes to its baseline configurations and documented and detected unauthorized changes, and will end on [REDACTED] the date [REDACTED] committed to complete its Mitigation Plan.

Aggregate Contributing Causes for CIP-010-2 R2 Alleged Violations

802. The primary cause of the CIP-010-2 R2 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the configuration monitoring process and implemented stronger internal controls to help ensure that the process was sufficient and followed. However, [REDACTED] process did not require and there were no internal controls to ensure that specific actions required by the process were followed. For instance, there were no controls to verify the accuracy of the firewall lists, which

are used to create the baseline configurations. Additional training, along with clearer instructions for completing tasks, could have helped prevent the Alleged Violations.

Aggregate Risk Statement of CIP-010-2 R2 Alleged Violations

803. The Regions determined that the Alleged Violations posed an aggregate moderate risk¹⁵² to the reliability of the Bulk Power System based on the following factors.¹⁵³ The risk posed was providing the opportunity for undetected changes to the baseline configurations, which could adversely impact BCSs. Notwithstanding, the subject devices were protected inside a 24/7 monitored Physical Security Perimeter. Further, all devices, except for the issues involving asset identification in the last Alleged Violation, were protected within a secured Electronic Security Perimeter.
804. Several factors increased the aggregate risk. In the first Alleged Violation, [REDACTED] failed to monitor for changes to its baseline configurations for [REDACTED] EACMSs at least once every 35-calendar days. The EACMSs were associated with high impact BES Cyber Systems. The Regions determined that [REDACTED] had serious, systemic security and compliance issues across its [REDACTED] functional groups, which required [REDACTED] to overhaul its entire CIP compliance program. Because of this, the risk for continued noncompliance and compromise to BCSs and CAs dramatically increased. Second, due to the weaknesses in [REDACTED] CIP compliance program, the Regions anticipate that [REDACTED] will identify additional instances of noncompliance while completing mitigation, which [REDACTED] will report to the Regions. Notwithstanding, [REDACTED] comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that [REDACTED] reports.

Mitigating Actions for CIP-010-2 R2 Alleged Violations

805. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-010-2 R2 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
806. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures;

¹⁵² Alleged Violation [REDACTED], individually posed a moderate risk to the reliability of the BPS, and [REDACTED] individually, posed a minimal risk.

¹⁵³ CIP-010-2 P2.1 has a VRF of “Medium” pursuant to CIP-010-2 Table of Compliance Elements. According to the VSL Matrix, these Alleged Violations warrant a “Severe” VSL.

(iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

807. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

KK. CIP-010-2 R3 [REDACTED]

808. CIP-010-2 prevents and detects 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 Bulk Electric System (BES).

809. CIP-010-2 R3 provides in relevant part:

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.

P3.1. At least once every 15 calendar months, conduct a paper or active vulnerability assessment.

....

P3.3. 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.

P3.4. 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 Alleged Violation for [REDACTED]

- 810. On September 2, 2016, [REDACTED] on behalf of [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-010-2 R3; P3.3. *See* Self-Report, **Attachment 39a**. [REDACTED] did not perform an active vulnerability assessment of a Protected Cyber Asset (PCA) prior to deploying them into the production environment.
- 811. On July 15, 2016, during a daily log review, [REDACTED] [REDACTED] [REDACTED] discovered that on July 14, 2016, a [REDACTED] subject matter expert (SME) did not complete an active vulnerability assessment as part of change management prior to commissioning the single PCA into an Electronic Security Perimeter (ESP), which contained [REDACTED] Cyber Assets (CAs). [REDACTED] had initiated the appropriate change management tickets, which initiated the required asset commissioning tasks, but the SME commissioned the asset in the production ESP prior to completing the active vulnerability assessment.
- 812. The Alleged Violation started on July 14, 2016, when the SME commissioned a PCA to the production ESP without first completing an active vulnerability assessment, and ended on July 20, 2016, when [REDACTED] removed the device from the ESP.

Description of Alleged Violation for [REDACTED]

- 813. During a Compliance Audit conducted [REDACTED] [REDACTED], the Regions determined that [REDACTED] as a [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED] was in violation of CIP-010-2 R3; P3.3. *See* PV Audit Summary, **Attachment 39b**. [REDACTED] did not perform an active vulnerability assessment of [REDACTED] CAs prior to deploying them into the production environment.
- 814. From a sampling of BES Cyber Assets (BCAs), the Regions determined that [REDACTED] placed [REDACTED] Electronic Access Control and Monitoring Systems (EACMs) firewall appliances into the production environment without performing an active vulnerability assessment.
- 815. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on July 12, 2016, when [REDACTED] completed the vulnerability assessment on the CAs.

Description of Alleged Violation for [REDACTED]