

May 30, 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]
FERC Docket No. NP19-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty¹ regarding noncompliance by [REDACTED] (the Entity), NERC Registry ID# [REDACTED],² with information and details regarding the nature and resolution of the violations³ discussed in detail in the Settlement Agreement attached hereto (Attachment 1), 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)).⁴

NERC is filing this Notice of Penalty with the Commission because [REDACTED] and the Entity have entered into a Settlement Agreement to resolve all outstanding issues arising from [REDACTED] determinations and findings of the violations of

¹ Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation, Docket No. RM05-30-000 (February 7, 2008). See also 18 C.F.R. Part 39 (2017). Mandatory Reliability Standards for the Bulk-Power System, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). See 18 C.F.R. § 39.7(c)(2).

² The Entity was included on the NERC Compliance Registry as a [REDACTED]

³ For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

⁴ See 18 C.F.R. § 39.7(c)(2) and 18 C.F.R. § 39.7(d).

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

NERC Notice of Penalty
The Entity
May 30, 2019
Page 2

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

CIP-004-6, CIP-005-5, CIP-006-3c, CIP-006-6, CIP-007-3a, CIP-007-6, CIP-010-2, and CIP-011-2. The Entity agreed to the \$1,000,000 monetary penalty [REDACTED] 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.

Statement of Findings Underlying the Violations

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

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2019), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. 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*	Violation Start-End Date	Risk	Penalty Amount
[REDACTED] 2017018032	CIP-004-6	R3; 3.4	Medium/ Severe	[REDACTED]	CA [REDACTED]	7/1/2016- 2/28/2018	Minimal	\$1M
[REDACTED] 2017018036	CIP-004-6	R4; 4.1	Medium/ Severe	[REDACTED]	CA [REDACTED]	7/6/2016	Minimal	
[REDACTED] 2017018037	CIP-005-5	R1; 1.3	Medium/ Severe	[REDACTED]	CA [REDACTED]	7/1/2016- 9/18/2018	Moderate	
[REDACTED] 2017018039	CIP-006-3c	R1; 1.6.1	Medium/ Severe	[REDACTED]	CA [REDACTED]	3/1/2015- 12/15/2017	Minimal	
[REDACTED] 2017018038	CIP-006-6	R1; 1.3	Medium/ Severe	[REDACTED]	CA [REDACTED]	12/7/2016- 10/31/2017	Minimal	
[REDACTED] 2017018040	CIP-007-3a	R2	Medium/ Severe	[REDACTED]	CA	12/19/2013- 8/17/2018	Serious	

5 [REDACTED]

NERC Notice of Penalty
The Entity
May 30, 2019
Page 3

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

NERC Violation ID	Standard	Req.	VRF/VSL	Applicable Function(s)	Discovery Method*	Violation Start-End Date	Risk	Penalty Amount
2017018043	CIP-007-3a	R3	Lower/ Severe		CA	12/19/2013-9/28/2018	Serious	
2017018044	CIP-007-6	R3	Medium/ Severe		CA	7/1/2016-8/17/2018	Serious	
2017018046	CIP-007-3a	R5	Medium/ Severe		CA	12/19/2013-12/31/2018	Serious	
2017018045	CIP-007-6	R4	Lower/ Severe		CA	7/1/2016-8/17/2018	Serious	
2017018047	CIP-010-2	R2	Medium/ Severe		CA	7/1/2016-2/28/2018	Minimal	
2017018048	CIP-011-2	R1	Medium/ Severe		CA	7/1/2016-4/25/2018	Moderate	

Background to the Violations

[REDACTED]

The Entity and [REDACTED] entered into a Settlement Agreement to resolve 12 violations of the CIP Reliability Standards. These violations were discovered during a Federal Energy Regulatory Commission (FERC) Compliance Audit [REDACTED]

[REDACTED] Following the FERC-led Compliance Audit, [REDACTED] initiated the processing of 12 violations of the CIP Reliability Standards.

[REDACTED]

NERC Notice of Penalty
The Entity
May 30, 2019
Page 4

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

[REDACTED]

[REDACTED]

[REDACTED] determined [REDACTED], the Entity was in violation of CIP Reliability Standards in multiple areas of security and compliance. The Entity also had issues with personnel and training, configuration change management and vulnerability assessments, and information protection. For each violation, the Entity conducted an extent of condition review to determine the scope, root causes, and contributing causes. The root cause of the violations was inadequate processes and procedures.

CIP-004-6 R3

[REDACTED] determined that [REDACTED] did not implement a personnel risk assessment (PRA) program that included a process or criteria or verifying that PRAs performed by contractors were conducted.

The root cause of this violation was inadequate procedures. The [REDACTED] only verified the completion of the PRA through a signed affidavit by the contractor conducting the PRA, but [REDACTED] was not actively involved in the assessment criteria or results of PRAs conducted by contractors.

[REDACTED] determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Attachment 3 includes the facts regarding the violation that [REDACTED] considered in its risk assessment.

The Entity submitted a Mitigation Plan to address the referenced violation. Attachment 3 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 3a

NERC Notice of Penalty
The Entity
May 30, 2019
Page 5

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

The Entity certified completion of the Mitigation Plan. [REDACTED] verified the Entity completed the Mitigation Plan as of February 28, 2018. Attachments 3b and 3c provide specific information on verification of the Entity's completion of the activities.

CIP-004-6 R4

[REDACTED] determined [REDACTED] did not have sufficient controls over the distribution of physical keys which led to the improper provisioning of a physical key to an employee without authorization.

The root cause of this violation was insufficient procedures that lacked specific details on how to manage physical access keys.

[REDACTED] determined the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. Attachment 3 includes the facts regarding the violation that [REDACTED] considered in its risk assessment.

The Entity submitted a Mitigation Plan to address the referenced violation. Attachment 3 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 4a.

The Entity certified completion of the Mitigation Plan. [REDACTED] verified the Entity completed the Mitigation Plan by March 5, 2018. Attachments 4b and 4c provide specific information on verification of the Entity's completion of the activities.

CIP-005-5 R1

[REDACTED] determined that [REDACTED] permitted Internet Control Message Protocol (ICMP) inbound and outbound communications through an Electronic Access Point (EAP) to its High and Medium Impact BCSs without maintaining documentation supporting the reason it granted the communication access.

The root cause was insufficient procedures that lacked the granularity necessary to ensure that access rules had need and reason clearly documented.

[REDACTED] determined the violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. Attachment 3 includes the facts regarding the violation that [REDACTED] considered in its risk assessment.

The Entity submitted a Mitigation Plan to address the referenced violation. Attachment 3 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 5a

NERC Notice of Penalty
The Entity
May 30, 2019
Page 6

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

The Entity certified completion of the Mitigation Plan.

CIP-006-3c R1

██████ determined that ██████████ did not maintain complete visitor access control logs for one facility containing high impact Bulk Electric system Cyber Systems (BCSs).

The root cause of this violation was inadequate process and oversight. ██████████ did not include periodic reviews to ensure compliance.

██████ determined the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. Attachment 3 includes the facts regarding the violation that ███████ considered in its risk assessment.

The Entity submitted a Mitigation Plan to address the referenced violation. Attachment 3 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 6a

The Entity certified completion of the Mitigation Plan. ███████ verified the Entity completed the Mitigation Plan by January 1, 2018. Attachments 6b and 6c provide specific information on verification of the Entity's completion of the activities.

CIP-006-6 R1

██████ determined that ██████████ did not implement two or more different physical access controls to restrict unescorted physical access into its ██████████ PSP.

The root cause of this violation was a lack of clarity in its physical security plan and inadequate procedures for how ██████████ should implement access control and management.

██████ determined the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. Attachment 3 includes the facts regarding the violation that ███████ considered in its risk assessment.

The Entity submitted a Mitigation Plan to address the referenced violation. Attachment 3 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 7a.

NERC Notice of Penalty
The Entity
May 30, 2019
Page 7

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

The Entity certified completion of the Mitigation Plan. [REDACTED] verified the Entity completed the Mitigation Plan by October 10, 2017. Attachments 7b and 7c provide specific information on verification of the Entity's completion of the activities.

CIP-007-3a R2

[REDACTED] determined that [REDACTED] did not properly document the need for enabled BES Cyber Asset (BCA) logical network accessible ports. Additionally, [REDACTED] did not provide evidence that a certain device had no provision for restricting or disabling ports.

The root cause of this violation was inadequate processes including a lack of controls to ensure it enabled only logical network accessible ports and services deemed necessary.

[REDACTED] determined the violation posed a serious risk to the reliability of the BPS. Attachment 3 includes the facts regarding the violation that [REDACTED] considered in its risk assessment.

The Entity submitted a Mitigation Plan to address the referenced violation. Attachment 3 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 8a.

The Entity certified completion of the Mitigation Plan.

CIP-007-3a R3

[REDACTED] determined that [REDACTED] did not assess security patches prior to deployment into the production environment.

The root cause was a lack of adequate processes and controls around the evaluation of security patches.

[REDACTED] determined the violation posed a serious and substantial risk to the reliability of the BPS. Attachment 3 includes the facts regarding the violation that [REDACTED] considered in its risk assessment.

The Entity submitted a Mitigation Plan to address the referenced violation. Attachment 3 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 9a.

CIP-007-6 R3

[REDACTED] determined that [REDACTED] did not implement a documented process to deter, detect, or prevent malicious code on Cyber Assets associated with High Impact BES Cyber Systems.

NERC Notice of Penalty
The Entity
May 30, 2019
Page 8

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

The root cause was inadequate processes and a lack of controls around the deployment of malware prevention protections.

██████ determined the violation posed a serious and substantial risk to the reliability of the BPS. Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted a Mitigation Plan to address the referenced violation. Attachment 3 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 10a

The Entity certified completion of the Mitigation Plan.

CIP-007-3a R5

██████ determined that ██████ did not identify all individuals with access to shared accounts. Additionally, where ██████ had Cyber Assets which could not limit unsuccessful authentication attempts to generate alerts after a threshold of unsuccessful authentication attempts, ██████ failed to document compensating measures in a filed technical feasibility exception (TFE).

The root causes were insufficient procedures that lacked specific details on how to manage access to system accounts and a lack of system access controls.

██████ determined the violation posed a serious and substantial risk to the reliability of the BPS. Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted a Mitigation Plan to address the referenced violation. Attachment 3 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 11a

The Entity certified completion of the Mitigation Plan.

CIP-007-6 R4

██████ determined that ██████ did not implement a process to log events for identification of, and after-the-fact investigations of, Cyber Security Incidents on Cyber Assets associated with High Impact BCSs.

The root causes were inadequate processes and a lack of controls around the event logging and generation of alerts.

NERC Notice of Penalty
The Entity
May 30, 2019
Page 9

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

████ determined the violation posed a serious and substantial risk to the reliability of the BPS. Attachment 3 includes the facts regarding the violation that █████ considered in its risk assessment.

The Entity submitted a Mitigation Plan to address the referenced violation. Attachment 3 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 12a.

The Entity certified completion of the Mitigation Plan.

CIP-010-2 R2

████ determined that █████ did not have documented processes for investigating detected unauthorized changes to its baseline configurations.

The root cause was a lack of documented steps for documenting or investigating detected unauthorized changes.

████ determined the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. Attachment 3 includes the facts regarding the violation that █████ considered in its risk assessment.

The Entity submitted a Mitigation Plan to address the referenced violation. Attachment 3 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 13a

The Entity certified completion of the Mitigation Plan. █████ verified the Entity completed the Mitigation Plan by February 28, 2018. Attachments 13b and 13c provide specific information on verification of the Entity's completion of the activities.

CIP-011-2 R1

████ determined that █████ did not verify a storage area network (SAN), used to store security configurations of its BCAs, as a Bulk Electric System Cyber System Information (BCSI) repository.

The root cause was a lack of documented methodology that included a detailed assessment to account for all locations that may contain BCSI.

NERC Notice of Penalty
The Entity
May 30, 2019
Page 11

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

Statement Describing the Assessed Penalty, Sanction, or Enforcement Action Imposed⁷

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,⁸ the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on May 7, 2019 and approved the resolution between [REDACTED] and the Entity. 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.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of [REDACTED] one million dollar (\$1,000,000) penalty is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Request for Confidential Treatment

For the reasons discussed below, NERC is requesting nonpublic treatment of certain portions of this filing pursuant to Sections 39.7(b)(4) and 388.113 of the Commission's regulations. This filing contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. As discussed below, this information, if released publically, would jeopardize the security of the Bulk Power System and could be useful to a person planning an attack on Critical Electric Infrastructure. NERC respectfully requests that the Commission designate the redacted portions of the Notice of Penalty as non-public and as Critical Energy/Electric Infrastructure Information ("CEII"), consistent with Sections 39.7(b)(4) and 388.113, respectively.⁹

⁷ See 18 C.F.R. § 39.7(d)(4).

⁸ *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

⁹ 18 C.F.R. § 388.113(e)(1).

NERC Notice of Penalty
The Entity
May 30, 2019
Page 12

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

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

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

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

Consistent with its past practice, NERC is redacting information from this Notice of Penalty according to Section 39.7(b)(4) because it contains information that would jeopardize the security of the BPS if publicly disclosed.¹⁰ The redacted information includes details that could lead to identification of the Entity, and information about the security of the Entity's systems and operations, such as specific processes, configurations, or tools the Entity uses to manage its cyber systems. As the Commission has previously recognized, information related to CIP violations and cyber security issues, including the identity of the Entity, may jeopardize BPS security, asserting that "even publicly identifying which entity has a system vulnerable to a 'cyber attack' could jeopardize system security, allowing persons seeking to do harm to focus on a particular entity in the Bulk-Power System."¹¹

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

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

¹⁰ 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); FOIA No. FY19-019 Determinations on Docket Nos. NP14-32 and NP14-41 (February 28, 2019); FOIA No. FY19-030, Determination on Docket No. NP10-132 (April 26, 2019). 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.

¹¹ *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).

¹² See the next section for a list of this information.

¹³ See below for a list of this information.

NERC Notice of Penalty
The Entity
May 30, 2019
Page 13

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

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

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

The Entity's systems and assets. The information also describes strategies, techniques, technologies, and solutions used to resolve specific cyber security issues.

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

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

NERC Notice of Penalty
The Entity
May 30, 2019
Page 14

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

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, May 30, 2019. Details about The Entity's operations, networks, and security should be treated and evaluated separately from its identity to avoid unnecessary disclosure of CEII that could pose a risk to security. NERC requests that the CEII designation apply to the redacted information from Items 3-9 for three years from this filing date, May 30, 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. Compliance monitoring of The Entity to ensure sustainability of the improvements described in this Notice of Penalty; and
2. Remediation of any subsequent violations discovered through compliance monitoring by the Regions.

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

Attachments to be Included as Part of this Notice of Penalty

The attachments to be included as part of this Notice of Penalty are the following documents:

1. Settlement Agreement by and between [REDACTED] and The Entity executed April 23, 2019, included as Attachment 1;
2. FERC Final Audit Report dated June 8, 2017, included as Attachment 2;
3. The Entity's Mitigation Plan designated as [REDACTED] MIT013657 for CIP-004-6 R3 submitted February 22, 2018, included as Attachment 3a;
4. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R3 submitted May 23, 2018, included as Attachment 3b;
5. Verification of Mitigation Plan Completion for CIP-004-6 R3 dated August 28, 2018, included as Attachment 3c.
6. The Entity's Mitigation Plan designated as [REDACTED] MIT013930 for CIP-004-6 R4 submitted June 19, 2018, included as Attachment 4a;
7. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R4 submitted July 20, 2018, included as Attachment 4b;

NERC Notice of Penalty
The Entity
May 30, 2019
Page 15

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

8. Verification of Mitigation Plan Completion for CIP-004-6 R4 dated August 16, 2018, included as Attachment 4c.
9. The Entity's Mitigation Plan designated as [REDACTED] MIT013916 for CIP-005-5 R1 submitted May 30, 2018, included as Attachment 5a;
10. The Entity's Certification of Mitigation Plan Completion for CIP-005-5 R1 submitted September 18, 2018, included as Attachment 5b;
11. Verification of Mitigation Plan Completion for CIP-005-5 R1 dated May 9, 2019, included as Attachment 5c.
12. The Entity's Mitigation Plan designated as [REDACTED] MIT013907 for CIP-006-3c R1 submitted May 23, 2018, included as Attachment 6a;
13. The Entity's Certification of Mitigation Plan Completion for CIP-006-3c R1 submitted June 11, 2018, included as Attachment 6b;
14. Verification of Mitigation Plan Completion for CIP-006-3c R1 dated August 17, 2018, included as Attachment 6c.
15. The Entity's Mitigation Plan designated as [REDACTED] MIT013658 for CIP-006-6 R1 submitted February 22, 2018, included as Attachment 7a;
16. The Entity's Certification of Mitigation Plan Completion for CIP-006-6 R1 submitted May 18, 2018, included as Attachment 7b;
17. Verification of Mitigation Plan Completion for CIP-006-6 R1 dated August 17, 2018, included as Attachment 7c.
18. The Entity's Mitigation Plan designated as [REDACTED] MIT013928 for CIP-007-3a R2 submitted June 4, 2018, included as Attachment 8a;
19. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R2 submitted August 17, 2018, included as Attachment 8b;
20. Verification of Mitigation Plan Completion for CIP-007-3a R2 dated May 9, 2019, included as Attachment 8c.
21. The Entity's Mitigation Plan designated as [REDACTED] MIT013929 for CIP-007-3a R3 submitted June 7, 2018, included as Attachment 9a;
22. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R3 submitted February 28, 2019, included as Attachment 9b;
23. Verification of Mitigation Plan Completion for CIP-007-3a R3 dated May 9, 2019, included as Attachment 9c.

NERC Notice of Penalty
The Entity
May 30, 2019
Page 16

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

24. The Entity's Mitigation Plan designated as [REDACTED] MIT013917 for CIP-007-6 R3 submitted May 30, 2018, included as Attachment 10a;
25. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R3 submitted August 17, 2018, included as Attachment 10b;
26. Verification of Mitigation Plan Completion for CIP-007-6 R3 dated May 9, 2019, included as Attachment 10c.
27. The Entity's Mitigation Plan designated as [REDACTED] MIT013931 for CIP-007-3a R5 submitted June 19, 2018, included as Attachment 11a;
28. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R5 submitted December 31, 2018, included as Attachment 11b;
29. Verification of Mitigation Plan Completion for CIP-007-3a R5 dated May 9, 2019, included as Attachment 11c.
30. The Entity's Mitigation Plan designated as [REDACTED] MIT013918 for CIP-007-6 R4 submitted May 30, 2018, included as Attachment 12a;
31. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R4 submitted August 17, 2018, included as Attachment 12b;
32. Verification of Mitigation Plan Completion for CIP-007-6 R4 dated May 9, 2019, included as Attachment 12c.
33. The Entity's Mitigation Plan designated as [REDACTED] MIT013908 for CIP-010-2 R2 submitted May 23, 2018, included as Attachment 13a;
34. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R2 submitted May 29, 2018, included as Attachment 13b;
35. Verification of Mitigation Plan Completion for CIP-010-2 R2 dated August 21, 2018, included as Attachment 13c.
36. The Entity's Mitigation Plan designated as [REDACTED] MIT013909 for CIP-011-2 R1 submitted May 23, 2018, included as Attachment 14a;
37. The Entity's Certification of Mitigation Plan Completion for CIP-011-2 R1 submitted August 8, 2018, included as Attachment 14b;
38. Verification of Mitigation Plan Completion for CIP-011-2 R1 dated May 9, 2019, included as Attachment 14c.

NERC Notice of Penalty
The Entity
May 30, 2019
Page 17

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

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

*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.

Edwin G. Kichline*
Senior Counsel and Director of
Enforcement Oversight
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

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

NERC Notice of Penalty
The Entity
May 30, 2019
Page 18

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

Conclusion

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

Respectfully submitted,

/s/ Alexander Kaplen

Edwin G. Kichline*

Senior Counsel 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

edwin.kichline@nerc.net

alexander.kaplen@nerc.net

cc: The Entity



Attachment 1

Settlement Agreement by and between [REDACTED] and
The Entity executed April 23, 2019

SETTLEMENT AGREEMENT

BETWEEN [REDACTED]

AND
[REDACTED]

I. INTRODUCTION

1. [REDACTED] and [REDACTED] (or Entity) (collectively Parties) enter into this Settlement Agreement (Agreement) to resolve violations¹ by the Entity of the below-referenced Reliability Standards and Requirements.²

Reliability Standard	Requirement	[REDACTED] Tracking No.	NERC Tracking No.
CIP-004-6	R3, Part 3.4	[REDACTED] 402755	[REDACTED]
CIP-004-6	R4, Part 4.1	[REDACTED] 402783	[REDACTED]
CIP-005-5	R1, Part 1.3	[REDACTED] 402784	[REDACTED]
CIP-006-3c	R1.6.1	[REDACTED] 402786	[REDACTED]
CIP-006-6	R1, Part 1.3	[REDACTED] 402785	[REDACTED]
CIP-007-3a	R2	[REDACTED] 402787	[REDACTED]
CIP-007-3a	R3	[REDACTED] 402790	[REDACTED]
CIP-007-6	R3	[REDACTED] 402791	[REDACTED]
CIP-007-3a	R5	[REDACTED] 402793	[REDACTED]
CIP-007-6	R4	[REDACTED] 402792	[REDACTED]
CIP-010-2	R2	[REDACTED] 402794	[REDACTED]
CIP-011-2	R1	[REDACTED] 402795	[REDACTED]

2. The Parties stipulate to the facts in this Agreement for the sole purpose of resolving the violations. The Entity neither admits nor denies that these facts constitute violations of the above-referenced Reliability Standard Requirements.

II. OVERVIEW OF [REDACTED]

¹ For purposes of this Settlement Agreement, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

² This Agreement references the version of the Reliability Standard in effect at the time each violation began. The Entity, however, committed to perform mitigating actions to comply with the most recent version of each Reliability Standard Requirement.

3. [REDACTED]
4. [REDACTED]
5. [REDACTED]
6. [REDACTED]

III. EXECUTIVE SUMMARY

7. This Agreement resolves twelve (12) violations of Critical Infrastructure Protection (CIP) Reliability Standards related to the Entity.³ The Division of Reliability Standards and Security (DRSS) in the Office of Electric Reliability of the Federal Energy Regulatory Commission (FERC or the Commission) conducted a CIP Compliance Audit of [REDACTED]

³ The facts related to the violations are set forth in Attachment 1, which is incorporated herein by reference.

[REDACTED] Following the FERC-led Compliance Audit, [REDACTED] initiated the processing of 12 violations of CIP Reliability Standards by the Entity.

8. [REDACTED]
9. [REDACTED] the Entity was in violation of CIP Reliability Standards in multiple areas of security and compliance, most seriously in systems security management (CIP-007), including physical and electronic security. The Entity also had issues with personnel and training, configuration change management and vulnerability assessments, and information protection. Of the 12 violations, NERC determined that five posed a minimal risk to the BES, 2 posed a moderate risk to the BES, and five posed a serious and substantial risk to the BES.
10. The Entity drafted Mitigation Plans that address each violation and prevent recurrence. Overall, the Entity submitted 12 Mitigation Plans that collectively include over 150 milestones. For each violation, the Entity conducted an extent of condition review to determine the scope, root causes, and contributing causes. The Entity determined inadequate processes and procedures was the root cause for all of the violations.
11. [REDACTED]

IV. ADJUSTMENT FACTORS

12. In addition to the facts and circumstances stated above, [REDACTED] considered the following factors in its penalty determination:
Internal Compliance Program
13. [REDACTED] reviewed the Entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. The Entity has had a documented ICP since December 12, 2012, which includes components, processes, responsibilities, and training needed to ensure the Entity maintains compliance. However, in this case it did not effectively enable the Entity to prevent and detect the violations.

Cooperation

14. [REDACTED] considered the Entity's cooperation during the Agreement process and determined it was a neutral factor. The Entity timely provided responses to requests for information; however, the responses were sometimes unclear and required additional information to enable [REDACTED] to discern it.

Compliance History

15. When calculating the penalty for the violations at issue in this Agreement, [REDACTED] considered whether the facts of these violations constitute repetitive infractions. The Entity has prior violations of CIP-004-1 and CIP-004-3 R4, CIP-005-1 R2, CIP-007-1 R2, CIP-007-1 R3, CIP-007-1 R4, CIP-007-1 R5, and CIP-007-1 R6 that are similar to the current violations and constitute repeat conduct.

16. The Entity's relevant prior noncompliance with CIP-004-1 and CIP-004-3 R4 include:

i. [REDACTED]

ii. [REDACTED]

17. [REDACTED]

18. The Entity's relevant prior noncompliance with CIP-007-1 R2 includes:

i. [REDACTED]

ii. [REDACTED]

19. The Entity's relevant prior noncompliance with CIP-007-1 R3 includes

[REDACTED]

20. The Entity's relevant prior noncompliance with CIP-007-1 R4 includes

21. The Entity's relevant prior noncompliance with CIP-007-1 R5 includes

22. The Entity's relevant prior noncompliance with CIP-007-1 R6 includes

V. PENALTY

23. Based upon the foregoing, the Entity agreed to pay a monetary penalty of \$1,000,000,
24. The Entity shall remit the penalty payment to [REDACTED] via check or by wire transfer, to an account to be identified by [REDACTED] within thirty days after the Agreement is either approved by the Commission or by operation of law. [REDACTED] shall notify the Commission if the payment is not timely received.
25. If the Entity fails to remit the payment by the required date, interest payable to [REDACTED] will begin to accrue on the outstanding balance, pursuant to the Commission's regulations at 18 C.F.R. § 35.19a(a)(2)(iii) from the date that payment is due, and shall be payable in addition to the payment.

VI. ADDITIONAL TERMS

26. 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.
27. [REDACTED] shall report the terms of all settlements of compliance matters to the NERC Board of Trustee Compliance Committee (BOTCC). 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, the NERC BOTCC will either approve or reject this Agreement. If the NERC BOTCC rejects the Agreement, NERC will provide specific written reasons for such rejection and [REDACTED] will attempt to negotiate with the Entity a

revised settlement agreement that addresses the concerns. If a settlement cannot be reached, the enforcement process will continue to conclusion. If the NERC BOTCC approves the Agreement, NERC will (a) report the approved settlement to the Commission for review and approval by order or operation of law and (b) publicly post the violations and the terms provided for in this Agreement.

28. This Agreement binds the Parties upon execution, and may only be altered or amended by written agreement executed by the Parties. The Entity expressly waives its right to any hearing or appeal concerning any matter set forth herein, unless and only to the extent that the Entity contends that any NERC or Commission action constitutes a material modification to this Agreement.
29. [REDACTED] reserves all rights to initiate enforcement action against the Entity in accordance with the NERC Rules of Procedure in the event that the Entity fails to comply with any of the terms or conditions of this Agreement. The Entity retains all rights to defend against such action in accordance with the NERC Rules of Procedure.
30. The Entity 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 the Entity's 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 the Entity 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 the Entity consent to the use of this Agreement by any other party in any other action or proceeding.
31. The Entity 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 [REDACTED] enters into this Agreement in express reliance on the representations contained herein, as well as any other representations or information provided by the Entity to [REDACTED] during any Entity interaction with [REDACTED] relating to the subject matter of this Agreement.
32. Upon execution of this Agreement, the Parties stipulate that each violation addressed herein constitutes a violation. The Parties further stipulate that all required, applicable information listed in Section 5.3 of the Compliance Monitoring and Enforcement Program is included within this Agreement.
33. 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.
34. 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.

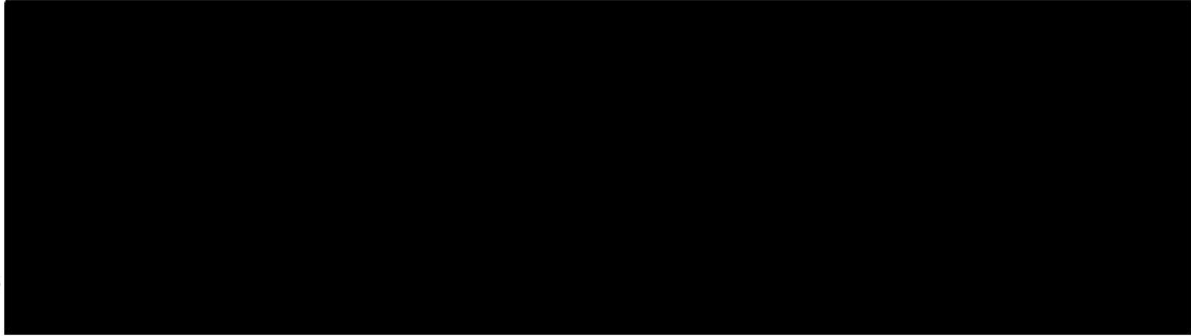
35. The Agreement may be signed in counterparts.
36. This Agreement is executed in duplicate, each of which so executed shall be deemed to be an original.

[SIGNATURE PAGE TO FOLLOW]⁴

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

⁴ An electronic version of this executed document shall have the same force and effect as the original.

Agreed to and accepted by:



Attachment A

I. VIOLATIONS

A. CIP-004-6 R3, Part 3.4 ([REDACTED])

1. CIP-004-6 R3 reduces the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment.
2. CIP-004-6 R3 states 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.
 - P3.1.** Process to confirm identity.
 - P3.2.** Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:
 - 3.2.1. current residence, regardless of duration; and
 - 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.

If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.

 - P3.3.** Criteria or process to evaluate criminal history records checks for authorizing access.
 - P3.4.** Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED]

3. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] [REDACTED] ([REDACTED]) was in violation of CIP-004-6 R3.⁵ The [REDACTED] [REDACTED] [REDACTED] did not properly retain required documentation of personnel risk assessments (PRAs). Additionally, [REDACTED] did not verify the

⁵ FERC, Final Audit Report, Docket No. PA16-7-000, [REDACTED] Designated Critical Energy/Electric Infrastructure Information (CEII).

Attachment A

performance of attestations associated with PRAs performed by contractors.

█████ later determined the Entity was specifically in violation of CIP-004-6 R3, Part 3.4.

4. The FERC audit team discovered instances where █████ failed to follow its documented procedure to acquire and retain documentation supporting the performance of PRAs conducted by its contractors. The documented program required █████ to obtain and retain an affidavit from the contractor company attesting that the contractor company had performed a required PRA for contractor personnel seeking CIP access.
5. █████
█████
█████
█████
█████
█████
6. However, █████ later determined that █████ did not implement a PRA program that included a process or criteria for verifying that PRAs performed by contractors were conducted according to CIP-004-6 R3, Parts 3.1 through 3.3. Under the PRA program, each contract company was responsible for completing a PRA for contractors it provided and █████ was responsible for obtaining an affidavit attesting to the successful completion of the PRA. However, █████ did not verify that contractor companies performed PRAs according to the requirements in CIP-004-6 R3, Parts 3.1 through 3.3 (as required by Part 3.4).
7. The root cause of this violation was inadequate procedures. █████ only verified the completion of the PRA through a signed affidavit by the contractor conducting the PRA, but █████ was not actively involved in the assessment criteria or results of PRAs conducted by contractors.
8. █████
█████
█████
9. The violation started on July 1, 2016, when the Standard became mandatory and enforceable on the Entity because prior versions of the Standard did not have a requirement to verify attestation results. The violation ended on February 28, 2018, when the Entity completed its Mitigation Plan.
10. NERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. █████ failure to implement a comprehensive procedure for contractor PRA completion could have permitted unqualified individuals with malicious intentions to obtain

Attachment A

authorized electronic access and authorized unescorted physical access to High Impact BCSs. This access could affect local operations through malicious actions and could potentially degrade the BPS. Even though [REDACTED] did not review any of the assessment results, it had supplemental terms and conditions with the contract agencies to ensure the PRAs were being performed. The total number of contractors working within the facilities containing High Impact BCSs was less than 15% of the total population ([REDACTED] contractors out of [REDACTED] individuals with access).⁶

Mitigating Actions for [REDACTED]

11. On February 22, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-004-6 R3, Part 3.4. On March 22, 2018, [REDACTED] accepted the Mitigation Plan
12. To mitigate this violation, the Entity:
 - i. developed an enterprise wide PRA procedure for verifying contractor and service vendor background checks and reviewed and revised, as needed, program documentation associated with PRAs for contractors and service vendors;
 - ii. developed and documented controls to ensure contractor and service vendor PRA process will be implemented as documented;
 - iii. developed a training program for contractor and service vendor PRAs;
 - iv. implemented updated PRA procedure;
 - v. based on the newly revised and implemented procedure for contractor and service vendor PRAs, conducted an extent of condition analysis. Specifically, the Entity identified all contractors and service vendors with CIP access and cross-checked to PRA evaluations. For all contractors and service vendors whose PRAs were not provided for assessment according to the newly implemented procedure, their CIP access was terminated until the PRA contents could be evaluated; and
 - vi. added a “training” section to the PRA procedure that defines who will be required to take training on the PRA process and why, as well as the periodicity for any refresher training. The Entity defined and documented both initial and refresher training requirements and incorporated this training into the enterprise-wide training program.
13. On May 23, 2018, the Entity certified to [REDACTED] that it completed the Mitigation Plan as of February 28, 2018. On August 10, 2018, [REDACTED] verified the Entity completed the Mitigation Plan by February 28, 2018.

B. CIP-004-6 R4, Part 4.1 ([REDACTED])

⁶ According to the CIP-004-6 Table of Compliance Elements, this noncompliance warranted a “Medium” VRF and a “Severe” VSL.

Attachment A

14. CIP-004-6 R4 reduces the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BCSs by requiring an access management program.
15. CIP-004-6 R4 states in relevant part:
 - 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:
 - 4.1.1. Electronic access;
 - 4.1.2. Unescorted physical access into a Physical Security Perimeter; and
 - 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED]

16. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] was in violation of CIP-004-6 R4. [REDACTED] later determined the Entity was specifically in violation of CIP-004-6 R4, Part 4.1. [REDACTED] did not have sufficient controls over the distribution of physical keys which led to the improper provisioning of a physical key to an employee without authorization.
17. The FERC audit team also found that [REDACTED] did not track or review access for the domain administrator accounts to Bulk Electric System Cyber System Information (BCSI). However, [REDACTED] later determined that the Entity's failure to track or review access to the domain accounts is a violation of CIP-007-6 R5 and should be addressed under NERC Violation ID: [REDACTED]
18. During the audit, the FERC audit team found the [REDACTED] for [REDACTED] (the individual responsible for distribution of physical access keys to individuals with authorized unescorted physical access), was not authorized for access to the Physical Security Perimeters (PSPs) that the physical access keys controlled. However, [REDACTED] later informed [REDACTED] that the [REDACTED] did have authorized unescorted access permissions for [REDACTED], which all contained High Impact BCSs.
19. [REDACTED] completed an EOC assessment for the physical access key controls. [REDACTED] identified one instance where the [REDACTED] had assigned a physical access key for facilities containing High Impact BCSs to an individual who the [REDACTED] had not authorized for unescorted physical access. The [REDACTED] provided a physical [REDACTED] key to an

Attachment A

unauthorized project manager employee to hand-deliver it to the IT systems administrator at the [REDACTED] which was [REDACTED] miles away. Approximately five hours later on the same day, the project manager delivered the key to the intended recipient, who had authorized unescorted access to the [REDACTED]

20. The [REDACTED] cited the primary root cause of this violation was insufficient procedures that lacked specific details on how to manage physical access keys.
21. The violation started on July 1, 2016, when the Standard became mandatory and enforceable on the Entity, and ended on March 5, 2018, when the Entity corrected the access and tracking issues, updated the procedures to prevent reoccurrence, and trained appropriate personnel.
22. [REDACTED] determined the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. [REDACTED] failure to properly assign and track keys used for physical access to facilities containing High Impact BCSs and BCSI could permit unauthorized individuals to obtain access and provide an opportunity for actions, either malicious or unintentional, to affect operations or BPS operations. However, any access made using a physical access override key at any site containing Medium or High Impact BCSs would result in a forced entry alarm to corporate security for immediate assessment. [REDACTED] erroneously provided a High Impact BCS physical key to only one individual. [REDACTED] subsequently retrieved the key without the individual accessing the High Impact BCS. The individual was an employee in good standing, with a valid PRA, who had been with [REDACTED] for over eleven years. Two months after this instance, [REDACTED] granted the individual authorized unescorted access to the [REDACTED]. Further, full time, armed security staff secured the facilities containing High Impact BCSs.⁷

Mitigating Actions for [REDACTED]

23. On June 19, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-004-6 R4, Part 4.1. On July 2, 2018, [REDACTED] accepted the Mitigation Plan.
24. To mitigate this violation, the Entity:
 - i. created a new role in the [REDACTED] for an 'Admin ID' within the Active Directory (AD) domain;
 - ii. removed "physical" keys from the power delivery [REDACTED] custodian who did not have authorized unescorted physical access to the PSPs. Documented by area, the transfer of "physical" keys to the area access managers

⁷ According to the CIP-004-6 Table of Compliance Elements, this noncompliance warranted a "Medium" VRF and a "Severe" VSL.

Attachment A

- (AAMs) in the area “physical” key control log. Compared AAM “physical” key control logs to [REDACTED] custodian “physical” key control log to ensure all “physical” keys are logged;
- iii. validated Information Technology (IT) “physical” key custodians, their “physical” key custodian roles, and the “physical” key distribution process. Ensured roles are created to manage IT “physical” keys. Validated IT “physical” key custodians have authorized unescorted physical access to the PSPs under their responsibility. Revised “physical” key authorizations and “physical” key distribution process;
 - iv. created separate roles in [REDACTED] for (1) CIP physical asset access; and (2) CIP Cyber Asset access. Verified that no CIP access role in [REDACTED] provides both physical and Cyber Asset access;
 - v. updated the “physical” key distribution procedure for [REDACTED] substations to require AAMs to verify that an individual has authorized unescorted access to a PSP before issuing a “physical” key. Trained [REDACTED] substation AAMs on the updated “physical” key distribution procedure;
 - vi. performed an EOC to validate the [REDACTED] and [REDACTED] substations “physical” key custodian process ensures that only individuals with authorized unescorted physical access are responsible for maintaining and issuing “physical” keys;
 - vii. held a training session on management’s expectations, responsibilities, and the updated procedure for managing access to “physical” keys with AAMs that are assigned [REDACTED] CIP access owner roles;
 - viii. verified that CIP access owner’s roles exist for IT, [REDACTED] and [REDACTED] substations in [REDACTED] for those responsible for managing “physical” keys. Created CIP access owner’s roles for “physical” keys in [REDACTED] and reported any additional discrepancies identified during verification to [REDACTED];
 - ix. trained “physical” key custodians on the responsibilities associated with [REDACTED] CIP access verification process for controlling “physical” keys;
 - x. revised and implemented the IT “physical” key control procedure used to manage IT owned Physical Security Perimeters (PSPs) and High Impact Control Centers;
 - xi. remediated any discrepancies found in the EOC performed to validate the [REDACTED] and [REDACTED] substations “physical” key custodian process;
 - xii. reviewed initial root causes identified during the development of the Mitigation Plan and verified that corrective measures had been implemented for root causes and contributing factors;
 - xiii. created an enterprise-wide “physical” key management process for Medium and High Impact PSPs; and
 - xiv. trained and implemented the newly created enterprise-wide “physical” key distribution documentation. Trained “physical” key custodians on the new enterprise-wide “physical” key distribution process. Implemented the new

Attachment A

enterprise-wide “physical” key distribution process and retired the individual business unit’s processes.

25. On July 20, 2018, the Entity certified to [REDACTED] that it completed the Mitigation Plan as of March 8, 2018. On August 16, 2018, [REDACTED] verified the Entity completed the Mitigation Plan by March 5, 2018.

C. CIP-005-5 R1, Part 1.3 ([REDACTED])

26. 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.
27. 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 – [ESP].
- P1.3.** Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED] 7

28. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] was in violation of CIP-005-5 R1. [REDACTED] later determined the Entity was specifically in violation of CIP-005-5 R1, Part 1.3. [REDACTED] permitted Internet Control Message Protocol (ICMP) inbound and outbound communications through an Electronic Access Point (EAP) to its High and Medium Impact BCSs without maintaining documentation supporting the reason it granted the communication access.
29. [REDACTED] used ICMP to communicate from within the Electronic Security Perimeter (ESP) to multiple external servers. [REDACTED] could not provide documentation supporting or documenting the need for having such outbound access permission enabled.
30. Using its CIP-002 BCS list, [REDACTED] initiated an EOC assessment to establish the scope of this violation for the specific ICMP aspect. [REDACTED] found it needed to disable the ICMP rule on [REDACTED] (14.06%) High and Medium Impact EAPS. [REDACTED] For those EAPs where [REDACTED] determined the ICMP to be necessary, [REDACTED] documented justification for the inbound and outbound access permissions.

Attachment A

31. The root cause of this violation was insufficient procedures that lacked the granularity necessary to ensure that access rules had need and reason clearly documented. A lack of clear guidance within the procedures allowed for multiple failures where [REDACTED] either did not address the potential access permissions on EAPs or managed the EAP configurations through their professional judgment and experience.
32. The violation started on July 1, 2016, when [REDACTED] enabled the ICMP through the EAP to High and Medium Impact BCSs. The violation was expected to end on or before September 18, 2018, when the Entity committed to complete its Mitigation Plan. [REDACTED] will verify the Entity's completion of the mitigating actions.
33. NERC determined the violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. [REDACTED] failure to document the need and reasons for inbound and outbound access permissions could permit individuals with malicious intent or through erroneous actions to implement protocols that could provide control aspects or mine data from within the ESP to the detriment of local operations or BPS functionality. However, [REDACTED] secured the Bulk Electric System Cyber Assets within an established Electronic Security Perimeter and PSP, both with real-time monitoring and alerting.⁸

Mitigating Actions for [REDACTED]

34. On May 30, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-005-5 R1, Part 1.3. On June 28, 2018, [REDACTED] accepted the Mitigation Plan.
35. To mitigate this violation, the Entity:
 - i. performed an EOC to mitigate ICMP non-compliance deficiencies identified in the audit report for Medium Impact BCS EAPs. Using the Responsible Entity's 1st Quarter 2017 CIP-002 BCS list, reviewed all EAPs for Medium Impact BCSs and ensured that implicit and/or configurable settings for ICMP access are disabled to the maximum extent possible. EAPs for Medium Impact BCSs that require ICMP to be enabled, documented the business or operational reason(s) ICMP access was granted. Reported any additional findings of ICMP non-compliance for Medium Impact BCS EAPs to [REDACTED];
 - ii. performed an EOC to mitigate ICMP non-compliance deficiencies identified in the audit report for High Impact BCS EAPs. Using the Responsible Entity's 1st Quarter 2017 CIP-002 BCS list, reviewed all

⁸ According to the CIP-005-5 Table of Compliance Elements, this noncompliance warranted a "Medium" VRF and a "Severe" VSL.

Attachment A

EAPs for High Impact BCSs and ensured that implicit and/or configurable settings for ICMP access are disabled to the maximum extent possible. EAPs for High Impact BCSs that require ICMP to be enabled, document the business or operational reason(s) ICMP access was granted. Reported any additional findings of ICMP non-compliance for High Impact BCS EAPs to [REDACTED];

- iii. updated the current EAP rule guidelines for Medium and High Impact BCSs. Enhanced the current EAP rule guidelines for Medium and High Impact BCSs, as necessary, as a single enterprise wide document. Identified EAP rules from the guidelines that are considered "high risk". Used the guidelines identified as "high risk" to perform an EOC of High Impact BCS EAP rules, of which the [REDACTED] BCSs are a subset;
- iv. performed an EOC to develop a complete inventory list of existing documentation, including policies, procedures, work instructions, drawings, implementation evidence templates (if applicable), and business justification for BCS EAP rules;
- v. performed an EOC analysis of all the High Impact BCS EAPs, which included those used in the performance of the [REDACTED] function, to identify "high risk", per the guidelines and developed a plan that prioritizes the mitigation of High Impact BCS EAPs;
- vi. performed an EOC to identify and document all inbound and outbound access permissions and denials and the associated business justification for all High and Medium Impact EAPs. This milestone is specific to Part 1.2;
- vii. performed an EOC to determine whether all High and Medium Impact BCAs, (and their associated PCAs), reside within an ESP, and all external connectivity is through an EAP that is identified on an ESP diagram. Using the Responsible Entity's 1st Quarter 2017 CIP-002 BCS list, confirmed that all applicable cyber assets reside within a defined ESP. Identified all EAPs on the ESP diagrams and checked that all BCA and PCA connectivity is through an EAP. This milestone is specific to Part 1.1 and Part 1.2;
- viii. working with the inventory list of existing documentation, IT determined how the evidence should be structured, and how the implementation evidence template will be a repeatable, sustainable process. Used the enterprise-wide templates to perform a consistent EOC across all BCS EAPs;
- ix. using the inventory list of inbound and outbound access permissions and denials and the guidance documentation and template(s) created, determined which firewall rules and business justifications, (inclusive of those related to temporary rules), meet the requirements listed within the guidance document. This milestone is specific to Part 1.3;
- x. using the identified BCS EAP inventory list for all High and Medium Impact BCS at Control Centers, performed an EOC to verify that there is

Attachment A

- at least one method of detecting malicious communication for all inbound and outbound communications. This milestone is specific to Part 1.5;
- xi. performed a root cause analysis to identify the actual root cause(s), addressing CIP-005-5 R1, Part 1.1 through Part 1.5;
 - xii. created comprehensive enterprise-wide policies, procedures and work instructions (including step-by-step instructions, documenting controls, malicious communication detection, guidelines, etc.) for current and new ESPs and/or devices. The documents address the steps to follow for compliance with all parts of Requirement R1 for all applicable High and Medium Impact BCAs (and their associated PCAs) as identified in the Responsible Entity's most recent CIP-002 BCS list;
 - xiii. developed training for new and updated documentation and implementation evidence templates, and provided training to personnel; and
 - xiv. communicated to all SMEs and users, information about the new or updated policies, procedures and work instructions.
36. To mitigate this violation, the Entity will correct any deficiency found in previous milestones.
37. On September 18, 2018, the Entity certified to [REDACTED] that it completed the Mitigation Plan as of September 18, 2018. [REDACTED] will verify the Entity's completion of the mitigating actions.

D. CIP-006-3c R1.6.1⁹ ([REDACTED])

38. CIP-006-3c ensures the management of physical access to Bulk Electric System (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.
39. CIP-006-3c R1.6.1 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:

⁹ The Entity's violation applies from Version 3c through Version 6 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained substantially the same in each version, with slight variations as follows. CIP-006-6 R2, Part 2.2 provides in relevant part:

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.

P2.2. 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.

Attachment A

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.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED]

40. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] was in violation of CIP-006-6 R2. [REDACTED] did not maintain complete visitor access control logs for one facility containing high impact Bulk Electric System Cyber Systems (BCSs). Specifically, the FERC audit team discovered several instances where [REDACTED] failed to record the exit time for visitors from the Physical Security Perimeter (PSP), as required by Part 2.2. [REDACTED] later determined this violation extended back to CIP-006-3c R1.6.1.
41. [REDACTED], shortly after the audit concluded, the [REDACTED] used its CIP-002 BCA and PSP lists and initiated an extent-of-condition assessment to establish the scope of this violation. Each business unit responsible for access at each specific facility assessed PSP visitor logs from between March 2015 to December 2016. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] The majority of the failures involved [REDACTED] failing to capture a.m. or p.m. and not documenting the exit time of the visitor.
42. The root cause of this violation was inadequate processes and oversight. The [REDACTED] did not include periodic reviews to ensure compliance.
43. The violation started on March 1, 2015, the first known date when [REDACTED] failed to properly log visitors, and ended on December 15, 2017, when the Entity completed its Mitigation Plan.
44. [REDACTED] determined the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. [REDACTED] failure to document visitor access and egress from the PSP could hinder any forensic investigation to a cyber security event or occurrence since it would be difficult to know who was within the PSP and had access to BCAs without proper record keeping. However, [REDACTED] did not identify any instances where visitor escorting was deficient. Visitor logs would be used for after the fact forensic

Attachment A

investigations and would not significantly impact the risk of an event occurring. [REDACTED] had controls implemented to prevent unauthorized physical access from occurring, including full-time armed security staff on site at its facilities containing high impact BCSs.¹⁰

Mitigating Actions for [REDACTED]

45. On May 23, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-006-6 R2. On June 22, 2018, [REDACTED] accepted the Mitigation Plan.
46. To mitigate this violation, the Entity:
 - i. evaluated the process for reviewing visitor access logs and identified enhancements to incorporate, including creating new controls and strengthening existing controls;
 - ii. reviewed process for signing visitors in and out of PSPs and identified enhancements to be incorporated, including creating new controls and strengthening existing controls;
 - iii. performed an EOC analysis by reviewing visitor log entries to all PSPs during the time period starting March 2015 to 4th quarter of 2016;
 - iv. modified and enhanced visitor log process for signing visitors in-and-out of PSPs;
 - v. reviewed the PSP visitor logs and identified all instances where the escort can correct deficient log entries missing required data and closed out the missing log entries; and
 - vi. scheduled and administered training with the employees and independent contractors who are responsible for monitoring, managing and reviewing visitor logs according to the revised processes.
47. On June 11, 2018, the Entity certified to [REDACTED] that it completed the Mitigation Plan as of December 15, 2017. On August 17, 2018, [REDACTED] verified the Entity completed the Mitigation Plan by January 1, 2018.

E. CIP-006-6 R1, Part 1.3 ([REDACTED])

48. CIP-006-6 ensures 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.
49. CIP-006-6 R1, Part 1.3 provides in relevant part:

¹⁰ CIP-006-3c R1.6 has a VSL of "Severe" according to the VSL Matrix and has a VRF of "Medium" pursuant to the VRF Matrix. Further, according to the CIP-006-6 Table of Compliance Elements, this noncompliance warranted a "Medium" VRF and a "Severe" VSL.

Attachment A

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.

P1.3. Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED]

50. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] was in violation of CIP-006-6 R1, Part 1.3. [REDACTED] did not implement two or more different physical access controls to restrict unescorted physical access into its [REDACTED] ([REDACTED]) PSP.
51. During the audit, FERC observed an emergency exit door permitted access into the [REDACTED] PSP when an emergency 'request-to-access' button on the exterior of the PSP door was pressed. The [REDACTED] contained High Impact BES Cyber Systems. However, to end this violation, [REDACTED] removed this door from the PSP description because the door at issue only provided access to an atrium area. Beyond the atrium area, the [REDACTED] was protected by two additional doors with two-factor authentication controlled access.
52. [REDACTED], shortly after the audit concluded, [REDACTED] used its CIP-002 BCS list and initiated an EOC assessment to establish the scope of this violation. [REDACTED] conducted a physical walk down of all PSPs to compare the design noted in the physical security plan to the actual, as built site. Specifically, at each PSP access point, [REDACTED] looked for any design that would allow someone to access a PSP through the activation of an emergency exit method from outside of the PSP egress door. [REDACTED] did not find any additional similar instances.
53. The root cause of this violation was a lack of clarity in its physical security plan and inadequate procedures for how [REDACTED] should implement access control and management, particularly in unique or complicated facilities.
54. The violation started on July 1, 2016, when the Standard became mandatory and enforceable on the Entity, and ended on October 31, 2017, when the Entity completed its Mitigation Plan.
55. [REDACTED] determined the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. [REDACTED] failure to properly configure an egress only request-to-exit option could have permitted an individual with malicious intentions to gain access into a PSP from the exterior

Attachment A

and impact local operations or affect operations of the BPS. However, [REDACTED] incorrectly identified the atrium area as a PSP, but since the area contains no BCSs or BCAs, it should not have been identified as a PSP. To remediate this issue, the [REDACTED] redefined the PSP and eliminated the atrium area from the PSP. The door at issue had a loud audible siren, which would sound when the request-to-exit button was activated. However, the area was not manned 24-7 which limited the siren's effectiveness. Other PSP doors with two factor access controls existed between the door at issue and the BCS or BCAs.¹¹

Mitigating Actions for [REDACTED]

56. On February 22, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-004-6 R4. On March 22, 2018, [REDACTED] accepted the Mitigation Plan.
57. To mitigate this violation, the Entity:
 - i. updated the PSP at the [REDACTED] site to remove the foyer area and removed the foyer door programming from the Physical Access Control Systems (PACS);
 - ii. revised the PSP drawing for the [REDACTED] to properly illustrate the foyer area and its authentication controls;
 - iii. reviewed each High Impact PSP design by conducting a walk down and ensured no entry by key core, push button, etc., into the PSP from an egress only door;
 - iv. corrected any egress only doors that allow entry into a High Impact PSP found during the walk down;
 - v. reviewed the enterprise-wide physical security plan to determine whether design expectations related to egress only doors are described within it;
 - vi. conducted training on the design expectations for egress only doors;
 - vii. revised facility security review procedure to include instructions that physical security drawings should be reviewed as part of a facility security review walk down, discussed with the business unit any changes or modifications that may have been made prior to the walk down, and documented exceptions identified during the walk down; and
 - viii. trained corporate security area security managers on the updated facility security review procedure.
58. On May 18, 2018, the Entity certified to [REDACTED] that it completed the Mitigation Plan as of October 31, 2017. On August 17, 2018, [REDACTED] verified the Entity completed the Mitigation Plan by October 10, 2017.

¹¹ According to the CIP-006-6 Table of Compliance Elements, this noncompliance warranted a "Medium" VRF and a "Severe" VSL.

Attachment A

F. CIP-007-3a R2¹² ([REDACTED])

59. CIP-007-3a ensures the management of system security by requiring Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).
60. CIP-007-3a R2 provides in relevant part:
- R2.** Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
- R2.1.** The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
- R2.2.** The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
- R2.3.** In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED]

61. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] was in violation of CIP-007-6 R1. [REDACTED] did not properly document the need for enabled BCA logical network accessible ports. Additionally, [REDACTED] did not provide evidence that a certain device had no provision for restricting or disabling ports. [REDACTED] later determined this violation extended back to Version 3a of the Standard and Requirement, when the Requirement was found at CIP-007-3a R2.
62. During the audit, the FERC audit team found that although [REDACTED] maintained a list of open of ports and services, it did not provide evidence of implementing any process or procedures for establishing whether there was a need for open ports. Additionally, the FERC audit team found that for a certain

¹² The Entity's violation applies from Version 3a through Version 6 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained mostly compatible between each version. 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.

P1.2. Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.

Attachment A

device that had no provision for disabling or restricting ports, [REDACTED] failed to provide evidence that the device had no provision for disabling or restricting ports.

63. Following the audit, [REDACTED] used its CIP-002 list of Medium and High Impact BCSs and initiated an EOC assessment to establish the scope of this violation. [REDACTED]
[REDACTED]
[REDACTED]
64. [REDACTED] determined that the root-cause of this violation was inadequate processes including a lack of controls to ensure it enabled only logical network accessible ports and services deemed necessary.
65. The violation began on December 19, 2013, when the audit period began, and ended on August 17, 2018, when the Entity completed its Mitigation Plan.
66. [REDACTED] determined the violation posed a serious risk to the reliability of the BPS. [REDACTED] failure to document the need and justification for all open ports and services could present an opportunity for unneeded and potentially vulnerable ports and services to be available for exploit by an individual with malicious intent. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] However, the [REDACTED] needed all the ports and services involved, but failed to document justification.¹³

Mitigating Actions for [REDACTED]

67. On June 4, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-007-6 R1. On July 2, 2018, [REDACTED] accepted the Mitigation Plan.
68. To mitigate this violation, the Entity:
- i. created an inventory list of policies, standards, procedures, and work instruction documentation for ports and services currently in effect for Information Technology (IT), [REDACTED] and [REDACTED]
[REDACTED] Business Units (BUs);

¹³ CIP-007-3a R2 has a VSL of "Severe" according to the VSL Matrix and has a VRF of "Medium" pursuant to the VRF Matrix. Further, according to the CIP-007-6 Table of Compliance Elements, this noncompliance warranted a "Medium" VRF and a "Severe" VSL.

Attachment A

- ii. developed an inventory list of all existing ports and services implementation evidence templates not previously identified for IT, [REDACTED] and [REDACTED] BUs;
- iii. determined the sustainability of existing ports and services implementation evidence templates in the inventory list for IT, [REDACTED] and [REDACTED] BUs. Decided how evidence should be structured, and how the ports and services implementation evidence templates can be used to create enterprise-wide ports and services evidence templates that are repeatable and sustainable;
- iv. evaluated the inventory list of effective policies, standards, procedures, and work instruction documentation for ports and services for IT, [REDACTED] and [REDACTED] BUs to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable and can be combined into corporate-wide documentation;
- v. performed an EOC, working with the 1st Quarter 2017 CIP-002 BES Cyber System list, determined if all enabled ports and services are documented for all applicable devices;
- vi. performed an EOC analysis to identify possible root cause(s);
- vii. performed a root cause analysis to determine root cause(s) and contributing factor(s);
- viii. developed a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the root cause analysis;
- ix. developed enterprise-wide documentation for ports and services, supplemented with processes regarding: (A) determination of devices for enabled ports and services; (B) documenting the need for enabled ports and services; (C) if a port and/or service cannot be disabled due to manufacturer constraints, document how the BU reaches out to the vendor to obtain evidence and document that this port and/or service as enabled.; (D) how the BUs determine if a Technical Feasibility Exception (TFE) is necessary for Part 1.1; and (E) how to protect against the use of unnecessary physical input/output ports;
- x. determined roles and responsibilities and identified ownership of devices by BU to ensure coverage for all ports and services;
- xi. the CIP Senior Manager and BU directors signed a letter agreeing to assigned ports and services responsibilities for specific inventoried devices, including training;
- xii. developed controls for ports and services documentation so that they are repeatable and sustainable;
- xiii. developed enterprise-wide implementation evidence templates for ports and services;
- xiv. developed training program for new and updated ports and services documentation and implementation evidence templates; and

Attachment A

- xv. performed training. Determined who is required to complete the training for ports and services, when and how often training is needed, how training will be scheduled and documented, and how completed training records will be stored and managed; and
 - xvi. implemented countermeasures, updated ports and services documentation, templates, and controls covering Part 1.1 and Part 1.2.
69. On August 17, 2018, the Entity certified to [REDACTED] that it completed the Mitigation Plan as of August 17, 2018. [REDACTED] will verify the Entity's completion of the mitigating actions.

G. CIP-007-3a R3¹⁴ ([REDACTED])

70. CIP-007-3a ensures the management of system security by requiring Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).
71. CIP-007-3a R3 provides in relevant part:
- R3.** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

¹⁴ The Entity's violation applies from Version 3a through Version 6 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained mostly compatible between each version. CIP-007-6 R2 provides in relevant part:

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.

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

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.

Attachment A

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.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED]

72. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] was in violation of CIP-007-6 R2. [REDACTED] did not assess security patches prior to deployment into the production environment. [REDACTED] later determined this violation extended back to Version 3a of the Standard and Requirement, when the Requirement was found at CIP-007-3a R3.
73. During the audit, the FERC audit team found [REDACTED] documented patch procedures required it to test the patches prior to applying them in the production environment. The FERC audit team found [REDACTED] did not provide evidence that it tested patches prior to deployment in the production environment. Further, the FERC audit team found [REDACTED] did not provide evidence that it tracked patches pursuant to its documented process.
74. Following the audit, [REDACTED] conducted an EOC assessment and identified additional instances where it failed to identify patching sources and failed to assess security patches. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
75. [REDACTED] indicated it did not have any additional documentation it wished to provide to demonstrate the assessment and testing of security patches, but maintained that it did not identify any instances where it deployed a patch without proper testing, either within an identified test environment or within sample devices in a similar production environment. [REDACTED] identified the root cause of this violation to be a lack of adequate processes and controls around the evaluation of security patches.

Attachment A

76. The violation began on December 19, 2013, when the audit period began, and is on-going. The violation was expected to end on or before September 28, 2018, when the Entity committed to complete its Mitigation. [REDACTED] will verify the Entity's completion of the mitigating actions.
77. [REDACTED] determined the violation posed a serious risk and substantial risk to the reliability of the bulk power system (BPS). [REDACTED] failure to assess all security patches could permit known security deficiencies to remain available for exploit and lead to actions that could be detrimental to the BPS. However, [REDACTED] had Electronic Security Perimeter firewalls protecting the Cyber Assets involved in this violation.¹⁵

Mitigating Actions for [REDACTED]

78. On June 7, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-007-6 R2. On July 2, 2018, [REDACTED] accepted the Mitigation Plan.
79. To mitigate this violation, the Entity:
- i. created an inventory list of policies, standards, procedures, and work instruction documentation for security patch management currently in effect for Information Technology (IT), [REDACTED] and [REDACTED] Business Units (BUs);
 - ii. developed an inventory list of all existing security patch management implementation evidence templates not previously identified for IT, [REDACTED] and [REDACTED] BUs;
 - iii. determined the sustainability of existing security patch management implementation evidence templates in the inventory list created for IT, [REDACTED] and [REDACTED] BUs. Decided how evidence should be structured, and how the security patch management implementation evidence templates can be used to create enterprise-wide security patch management evidence templates that are repeatable and sustainable;
 - iv. evaluated the inventory list created of effective policies, standards, procedures, and work instruction documentation for security patch management for IT, [REDACTED] and [REDACTED] BUs to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable and can be combined into corporate-wide documentation;
 - v. performed an EOC, working with the 1st Quarter 2017 CIP-002 BES [REDACTED], identified if there is documentation for the hardware and/or software patching requirements which involve monitoring of vendors for possible patches;

¹⁵ CIP-007-3a R3 has a VSL of "Severe" according to the VSL Matrix and has a VRF of "Lower" pursuant to the VRF Matrix. According to the CIP-007-6 Table of Compliance Elements, this noncompliance warranted a "Medium" VRF and a "Severe" VSL.

Attachment A

- vi. performed an EOC analysis to identify possible root cause(s). Reported any additional findings of non-compliance to [REDACTED];
 - vii. performed a root cause analysis to determine root cause(s) and contributing factor(s);
 - viii. developed a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the root cause analysis;
 - ix. determined roles and responsibilities. Identified ownership of devices by BU to ensure coverage;
 - x. the CIP Senior Manager and BU directors signed a letter agreeing to assigned compliance responsibilities for specific devices, including training;
 - xi. created enterprise-wide documentation, supplemented with processes regarding: (A) documenting contact with vendors every 35 calendar days on the availability of applicable security patches; (B) evaluation of security patches to include who performs the evaluation and the criteria used for determination; (C) creating and revising mitigation plans for security patches that cannot be applied within 35 calendar days after the patch evaluation; (D) applying security patches within 35 calendar days of evaluation; and (E) if there are network scans provided as evidence, where they are stored, and who does the scans;
 - xii. developed controls for the CIP-007-6 processes to make them repeatable and sustainable. For the enterprise-wide documentation developed, documented controls for creating and maintaining all processes;
 - xiii. created enterprise-wide implementation evidence templates, including: (A) a section for contact with vendors for applicable security patches every 35 calendar days; (B) a section to track the evaluation results of security patches, showing completion dates within 35 calendar days of being notified of a security patch release; (C) documentation that security patches were applied within 35 calendar days of evaluation; and (D) details of the mitigation plan;
 - xiv. developed training program for new and updated documentation and implementation evidence templates. Developed an enterprise-wide training program for when documentation and/or implementation evidence templates are created or updated; and
 - xv. performed training. Determined who is required to complete the training, when and how often training is needed, how training will be scheduled and documented, and how completed training records will be stored and managed.
80. To mitigate this violation, the Entity will implement new and/or updated CIP-007-6 documentation and controls and the BUs will submit implementation evidence for each Part of CIP-007-6 R2.

Attachment A

81. The Entity will certify to [REDACTED] once it completes the Mitigation Plan. The expected completion date was September 28, 2018. [REDACTED] will verify the Entity's completion of the mitigating actions.

H. CIP-007-6 R3¹⁶ ([REDACTED])

82. CIP-007-6 ensures the management of system security by specifying 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.

83. 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.

P3.2. Mitigate the threat of detected 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.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED]

84. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] was in violation of CIP-007-6 R3, Part 3.1. [REDACTED] did not implement a documented process to deter, detect, or prevent malicious code on Cyber Assets associated with High Impact BES Cyber Systems.
85. The FERC audit team found that [REDACTED] implemented a network system option through an intrusion detection and prevention system for the Cyber Assets that could not support Cyber Asset based malware prevention software. However, the two PACS and six EACMS identified by the FERC audit team were outside of the Electronic Security Perimeter (ESP), and [REDACTED] could not protect them with the network solution.

¹⁶ The Entity's violation applies from Version 3a through Version 6 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained mostly compatible between each version. CIP-007-6 R3, Part 3.1 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.

Attachment A

86. Following the audit, [REDACTED] completed an EOC assessment and identified additional instances where it did not provide malware prevention protection for all applicable systems.
87. For the [REDACTED] function, [REDACTED] identified three instances where malware prevention was absent, antivirus was absent, or both were absent affecting all [REDACTED] BCAs, all [REDACTED] PCAs, and all [REDACTED] EACMS, and one instance where malware prevention and antivirus was absent affecting [REDACTED] PACS.
88. [REDACTED] identified the root cause of this violation to be inadequate processes and a lack of controls around the deployment of malware prevention protections. Where [REDACTED] did not utilize Cyber Asset level malware prevention at the suggestion of device vendors, [REDACTED] also did not research or utilize a BES Cyber System approach for malware prevention.
89. The violation began on July 1, 2016, when the Standard became mandatory and enforceable on the Entity, and ended on August 17, 2018, when the Entity completed its Mitigation Plan.
90. [REDACTED] determined the violation posed a serious and substantial risk to the reliability of the BPS. [REDACTED] failure to provide anti-virus and malware prevention protection for some Cyber Assets outside of the established ESP could have resulted in any of the involved Cyber Assets becoming corrupted and compromised, leaving [REDACTED] operations in jeopardy and potentially affecting the operation and resilience of the BPS. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Mitigating Actions for [REDACTED]

91. On May 30, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-007-6 R3, Part 3.1. On June 28, 2018, [REDACTED] accepted the Mitigation Plan.
92. To mitigate this violation, the Entity:
- created an inventory list of policies, standards, procedures, and work instruction documentation for malicious code prevention currently in effect for Information Technology (IT), [REDACTED] and [REDACTED]
[REDACTED] Business Units;

¹⁷ CIP-007-3a R4 has a VSL of "Severe" according to the VSL Matrix and has a VRF of "Medium" pursuant to the VRF Matrix. Further, according to the CIP-007-6 Table of Compliance Elements, this noncompliance warranted a "Medium" VRF and a "Severe" VSL.

Attachment A

- ii. developed an inventory list of all existing malicious code prevention implementation evidence templates not previously identified for IT, [REDACTED] and [REDACTED] BUs;
- iii. determined the sustainability of existing malicious code prevention implementation evidence templates in the inventory list for IT, [REDACTED] and [REDACTED] BUs. Decided how evidence should be structured, and how the malicious code prevention implementation evidence templates can be used to create enterprise-wide malicious code prevention evidence templates that are repeatable and sustainable;
- iv. evaluated the inventory list of effective policies, standards, procedures, and work instruction documentation for malicious code prevention for IT, [REDACTED] and [REDACTED] BUs to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable;
- v. performed an EOC, working with the 1st Quarter 2017 CIP-002 BES Cyber System list, confirmed there is documentation based on device type for devices capable of detecting, deterring, or preventing malicious code;
- vi. performed an EOC analysis to identify possible root cause(s). Reported any additional findings of non-compliance to [REDACTED];
- vii. performed a root cause analysis to determine root cause(s) and contributing factor(s);
- viii. developed a list of sustainable countermeasures to the root cause(s) and contributing factors identified;
- ix. developed a technical and/or procedural solution for those devices that cannot deter, detect or prevent malicious code;
- x. created enterprise-wide documentation, supplemented with processes regarding: (A) how to protect devices from malicious code; (B) how to respond to malicious code detection; (C) how to mitigate the threat of malicious code; (D) how to transition into the Cyber Security Incident Response Plan, if malicious code is detected; (E) updating signatures or patterns; and (F) how and when to perform installations;
- xi. determined roles and responsibilities and identified ownership of devices by BU to ensure coverage;
- xii. developed controls for the CIP-007 processes to make them repeatable and sustainable. As part of the enterprise-wide documentation developed, documented controls for creating and maintaining all processes;
- xiii. the CIP Senior Manager and BU directors signed a letter agreeing to assigned compliance responsibilities for specific devices, including training;
- xiv. created enterprise-wide implementation evidence templates for capturing compliance evidence;
- xv. developed training program for new and updated documentation and implementation evidence templates;

Attachment A

- xvi. performed training. Determined who is required to complete the training, when and how often training is needed, how training will be scheduled and documented, and how completed training records will be stored and managed; and
- xvii. implemented new and/or updated CIP-007-6 documentation and controls. BUs submitted implementation evidence for each Part of the CIP-007-6 Requirement R3.

93. On August 17, 2018, the Entity certified to [REDACTED] that it completed the Mitigation Plan as of August 17, 2018. [REDACTED] will verify the Entity's completion of the mitigating actions.

I. CIP-007-3a R5¹⁸ CIP-007-6 R5 ([REDACTED])

94. CIP-007-3a ensures the management of system security by requiring Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).
95. CIP-007-3a R5 provides in relevant part:
- R5.** Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

¹⁸ The Entity's violation applies from Version 3a through Version 6 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained mostly compatible between each version. CIP-007-6 R5 provides in relevant part:

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 individuals who have authorized access to shared accounts.

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.

Attachment A

- 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.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED]

Attachment A

96. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] was in violation of CIP-007-6 R5. [REDACTED] did not identify all individuals with access to shared accounts, as required by Part 5.3. Additionally, where [REDACTED] had Cyber Assets which could not limit unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, the [REDACTED] failed to document compensating measures in a filed technical feasibility exception (TFE), as required by Part 5.7. [REDACTED] later determined that this violation extended back to Version 3a of the Standard.
97. The FERC audit team also found that [REDACTED] did not track access or review access for the domain administrator accounts to Bulk Electric System Cyber System Information (BCSI) and originally reported it as a possible violation of CIP-004-6 R4 (originally included under NERC Violation ID: [REDACTED]). However, [REDACTED] later determined that [REDACTED] failure to track access or review access to the domain accounts is a violation of CIP-007-6 R5, Part 5.2 and 5.3 and should be addressed under this NERC Violation ID: [REDACTED]. The identification of the domain accounts and users under CIP-007-6 R5, Part 5.2 and 5.3 precedes the authorization of need cited in CIP-004-6 R4, Part 4.1.
98. During the audit, the FERC audit team found that [REDACTED] excluded a shared domain account from the system it used to track account access. Therefore, the [REDACTED] did not follow its documented process to identify and track this account which had remote access to Cyber Systems and Assets, as required by Part 5.3. In August 2016, [REDACTED] added this shared domain account to its tracking system.
99. During the audit, the FERC audit team also found that [REDACTED] did not effectively track access authorizations or review access to its domain administrator accounts within its enterprise access management systems tool as required by Parts 5.2 and 5.3.
100. Following the audit, [REDACTED] completed an EOC assessment and identified additional instances where it did not track shared accounts and participation as required by Parts 5.2 and 5.3. For the [REDACTED] function specifically, there were [REDACTED] total domain administrator accounts, [REDACTED] of which were shared accounts among [REDACTED] individuals, and [REDACTED] individual accounts. Of these, [REDACTED] failed to track who had access to [REDACTED] (83.33%) of the accounts. [REDACTED] had various uses for the domain administrator accounts, including monitoring systems, infrastructure accounts, and accounts used to manage virtual desktops in various domains, etc. The untracked accounts had access to various Cyber Assets classified as BCAs, PCAs, and EACMs. The individuals with access to domain administrator accounts had a business need based on their job responsibilities.

Attachment A

101. During the audit, the FERC audit team found that for a certain device that did not support alerts for unsuccessful authentication attempts nor had a lock out feature, [REDACTED] failed to provide evidence of mitigating measures or a documented TFE covering the device, as required by Part 5.7.
102. Following the audit, as part of its EOC assessment, [REDACTED] considered whether documentation was available indicating which devices can limit the number of unsuccessful authentication attempts, or generate alerts after a threshold of unsuccessful authentication attempts. [REDACTED] found no additional instances of noncompliance with Part 5.7.
103. [REDACTED] cited the primary root cause of this violation as insufficient procedures that lacked specific details on how to manage access to system accounts and a lack of system access controls.
104. The violation began on December 19, 2013, when the audit period began, and is on-going. The violation was expected to end on or before December 31, 2018, when the Entity committed to complete its Mitigation.
105. [REDACTED] determined the violation posed a serious and substantial risk to the reliability of the BPS. [REDACTED] failure to track all accounts and individuals with access to shared accounts on High Impact BCSs could permit an individual with malicious intent to obtain access, initiate, or execute actions that would be detrimental to local operations or the BPS, and not be initially considered in any forensic investigation. Additionally, the EOC assessment revealed that [REDACTED] did not track multiple additional domain administrator accounts or the identification of individuals with access. In addition, the failure to file a TFE where Cyber Assets could not limit or alert on unsuccessful authentication attempts could permit Cyber Assets to go without some level of documented remediation or risk management controls and remain vulnerable to a brute force or denial-of-service attack. The failure to file a TFE portion of this violation involved just one device type and a small number of Cyber Assets where [REDACTED] did not file for a TFE.¹⁹

Mitigating Actions for [REDACTED]

106. On June 19, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-007-6 R5. On July 2, 2018, [REDACTED] accepted the Mitigation Plan.
107. To mitigate this violation, the Entity:
 - i. created an inventory list of policies, standards, procedures, and work instruction documentation for system access control currently in effect for

¹⁹ CIP-007-3a R5 has a VSL of “Severe” according to the VSL Matrix and R5.1, an impacted sub-requirement, has a VRF of “Medium” pursuant to the VRF Matrix. According to the CIP-007-6 Table of Compliance Elements, this noncompliance warranted a “Medium” VRF and a “Severe” VSL.

Attachment A

- Information Technology (IT), [REDACTED] and [REDACTED]
[REDACTED] Business Units;
- ii. developed an inventory list of all existing system access control implementation evidence templates not previously identified for IT, [REDACTED] and [REDACTED] BUs;
 - iii. determined the sustainability of existing system access control implementation evidence templates in the inventory list for IT, [REDACTED] and [REDACTED] BUs. Decided how evidence should be structured, and how the system access control implementation evidence templates can be used to create enterprise-wide system access control evidence templates that are repeatable and sustainable;
 - iv. evaluated the inventory list of effective policies, standards, procedures, and work instruction documentation for system access control for IT, [REDACTED] and [REDACTED] BUs to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable;
 - v. performed an EOC working with the 1st Quarter 2017 CIP-002 BES [REDACTED], evaluated system access control documentation for each device to validate if the requirements of CIP-007-6 R5, Part 5.1 through Part 5.7 are met;
 - vi. performed an EOC analysis to identify possible root cause(s);
 - vii. performed a root cause analysis to determine root cause(s) and contributing factor(s);
 - viii. developed a list of sustainable countermeasures to the root cause(s) and contributing factors identified;
 - ix. determined roles and responsibilities. Identified ownership of devices by BU to ensure coverage;
 - x. created enterprise-wide documentation, supplemented with processes regarding: (A) how interactive user access is authenticated; (B) how to determine if a TFE is required for when authentication of interactive user access cannot be enforced; (C) how to remove, rename or disable default or generic accounts on devices prior to placing into production; (D) documenting shared accounts and the individuals who have authorized access to shared accounts; (E) changing default passwords on devices prior to being placed into production; (F) enforcing password complexity, by determining whether technically or procedurally passwords are enforced based on device type; (G) enforcing password changes at least once every 15 calendar months; (H) how to determine if a TFE is required for when passwords cannot be changed on specific devices or device types every 15 calendar months; (I) how devices shall limit the number of unsuccessful authentication attempts, or generate alerts after a threshold of unsuccessful authentication attempts occurs; and (J) if devices are not capable of limiting the number of unsuccessful authentication attempts, or

Attachment A

- generating alerts after a threshold of unsuccessful authentication attempts, then document how the BU shall determine if a TFE is necessary;
- xi. the BUs developed controls for the CIP-007 processes to make them repeatable and sustainable. Controls for creating and maintaining all processes will be documented in the enterprise-wide documentation developed during the execution of Milestone 10;
 - xii. the CIP Senior Manager and BU Directors signed a letter agreeing to assigned compliance responsibilities for specific devices, including training;
 - xiii. created enterprise-wide implementation evidence templates for capturing compliance evidence;
 - xiv. reviewed and validated that all AD groups in the transmission domain have properly assigned roles;
 - xv. moved all transmission AD access from [REDACTED] to [REDACTED];
 - xvi. identified how the access control lists are determined across the various platform types and gathered the requirements needed to extract the data from target systems;
 - xvii. developed a training program for new and updated documentation and implementation evidence templates;
 - xviii. performed training. Determined who is required to complete the training, when and how often, how training will be scheduled and documented, and how completed training records will be stored and managed;
 - xix. performed an EOC, by identifying all CIP [REDACTED] devices and mapping all roles from the CIP [REDACTED] device to the access management system roles in [REDACTED]. Notified [REDACTED] of any compliance issues discovered;
 - xx. created a standardized enterprise-wide access matrix template with clearly defined roles;
 - xxi. implemented countermeasures and execute updated CIP-007 R5 documents and controls;
 - xxii. developed a mechanism for extracting and comparing the access management tool's users and roles to target system's access control list;
 - xxiii. performed an EOC by identifying all CIP [REDACTED] devices and mapping all roles from the CIP [REDACTED] device to the access management system roles in EAMS. Verify that access to CIP [REDACTED] devices is granted through access management roles. Create new roles if discrepancies are identified. Assign appropriate personnel to any new role once confirmed they are eligible and have a business need. Notify [REDACTED] of any compliance issues discovered;
 - xxiv. cleaned-up and restructure roles using the results of the above activities; and
 - xxv. created a new enterprise-wide access matrix and populate it with roles.

Attachment A

108. On December 31, 2018, the Entity certified to [REDACTED] that it completed the Mitigation Plan as of December 31, 2018. [REDACTED] will verify the Entity's completion of the mitigating actions.

J. CIP-007-6 R4 ([REDACTED])

109. CIP-007-6 ensures the management of system security by specifying 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.

110. CIP-007-6 R4 provides in relevant part:

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.

P4.2. 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.

P4.3. 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.

P4.4. 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.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED]

111. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] was in violation of CIP-007-6 R4. [REDACTED] did not implement a process to log events for identification of, and after-the-fact investigations of, Cyber Security Incidents on Cyber Assets associated with High Impact BCSs.

Attachment A

112. The FERC audit team found that for the two PACS and six EACMS that did not have the network intrusion detection and prevention software solution [REDACTED] [REDACTED] could not log malicious code detection events. The systems were outside of the ESP and [REDACTED] could not monitor and log events for them using the network solution.
113. Following the audit [REDACTED] completed an EOC assessment and identified additional instances where it did not provide event logging for all Cyber Assets.
114. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
115. Instances represent process gap categories, including no communication with [REDACTED] no antivirus installation, no intrusion detection system (IDS) protection, no antivirus and IDS logging and alerting, no logging for failed login and access attempts, no capability of sending logs for login and access attempts, or a combination of two or more gaps.
116. [REDACTED] identified the root cause of this violation to be inadequate processes and a lack of controls around the event logging and generation of alerts.
117. The violation began on July 1, 2016, when the Standard became mandatory and enforceable on the Entity, and ended on August 17, 2018, when the Entity completed its Mitigation Plan.
118. [REDACTED] determined the violation posed a serious and substantial risk to the reliability of the BPS. [REDACTED] failure to log Cyber Security Incidents could have resulted in a compromise of these Cyber Assets being unidentified and not responded to in a timely manner, leaving the network and operations vulnerable to more serious and compounding levels of degradation and risk. [REDACTED] [REDACTED] had all Cyber Asset within an established Electronic Security Perimeter behind a firewall. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

²⁰ CIP-007-3a R6 has a VSL of "Severe" according to the VSL Matrix and has a VRF of "Lower" pursuant to the VRF Matrix. According to the CIP-007-6 Table of Compliance Elements, this noncompliance warranted a "Medium" VRF and a "Severe" VSL.

Attachment A

Mitigating Actions for [REDACTED]

119. On May 30, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-007-6 R4. On June 28, 2018, [REDACTED] accepted the Mitigation Plan.
120. To mitigate this violation, the Entity:
- i. created an inventory list of policies, standards, procedures, and work instruction documentation for security event monitoring currently in effect;
 - ii. developed an inventory list of all existing security event monitoring implementation evidence templates;
 - iii. determined the sustainability of existing security event monitoring implementation evidence templates. Decided how evidence should be structured and how to use the security event monitoring implementation evidence templates to create enterprise-wide security event monitoring evidence templates that are repeatable and sustainable;
 - iv. evaluated the security event monitoring documentation and determined which content, instructions, and tools meet the Standard requirement, are repeatable and sustainable, and can be combined into corporate-wide documentation;
 - v. Working with the 1st Quarter 2017 CIP-002 BSC list, ensured there is documentation for the devices capable of logging and alerting on security events, to include detecting successful login attempts, failed access and login attempts, and malicious code; ensured there is documentation for the devices that can generate alerts for security events, when needed, and included alerts for detected malicious code and failure of event logging; ensured documentation for which devices are capable of retaining event logs for greater than 90 consecutive calendar days; and, ensured documentation associated with review of logged events every 15 calendar days to identify undetected cyber security incidents for High Impact BCSs and their associated EACMS and PCA;
 - vi. performed an EOC analysis to identify possible root cause(s) and contributing factors, using the inventory of documentation and devices identified during execution of activities described above. Compiles questions and performed interviews for additional input for the EOC analysis. Reported any additional findings of non-compliance to [REDACTED];
 - vii. performed a root cause analysis to determine root cause(s) and contributing factor(s).
 - viii. developed a list of sustainable countermeasures to the root cause(s) and contributing factors identified;

Attachment A

- ix. created enterprise-wide documentation including input from activity “iv” above and supplemented with processes for: (A) tracking log events at either the BCS level, or at the BES asset level (if there is no ability to log events at the BCS or BES asset level, require vendor documentation); (B) generating alerts for security events that require an alert; (C) retaining event logs for the last 90 consecutive calendar days and in the case of a CIP Exceptional Circumstance event, retaining logs longer than 90 consecutive calendar days; (D) how to determine if a TFE is necessary for when event logs cannot be retained for at least 90 consecutive calendar days; (E) review of sampled logged events at intervals no greater than 15-calendar days to identify undetected cyber security incidents; (F) suspicious activity that requires activation of the Cyber Security Incident Response Plan;
 - x. determined Roles and Responsibilities. Identified and documented business unit ownership of devices to ensure coverage for administering training;
 - xi. developed controls for the CIP-007 processes to make them repeatable and sustainable. Documented controls for creating and maintaining all processes for the enterprise-wide documentation;
 - xii. the CIP Senior Manager and BU Directors signed a letter agreeing to assigned compliance responsibilities for specific devices, including training;
 - xiii. created enterprise-wide implementation evidence templates for capturing compliance evidence;
 - xiv. developed a training program for new and updated documentation and implementation evidence templates;
 - xv. performed training and determined who is required to complete the training, when and how often training is needed, how training will be scheduled and documented, and how completed training records will be stored and managed; and
 - xvi. implemented new and/or updated CIP-007 documentation and controls and submitted implementation evidence for each Part of CIP-007 R4.
121. On August 17, 2018, the Entity certified to [REDACTED] that it completed the Mitigation Plan as of August 17, 2018. [REDACTED] will verify the Entity’s completion of the mitigating actions.

K. CIP-010-2 R2 ([REDACTED])

122. CIP-010-2 helps to prevent and detect 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).

Attachment A

123. CIP-010-2 R2 provides in relevant part:

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.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED]

124. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] was in violation of CIP-010-2 R2. [REDACTED] did not have documented processes for investigating detected unauthorized changes to its baseline configurations.
125. The FERC audit team found that while [REDACTED] had documented procedures for monitoring and documenting configuration changes, it did not have documented procedures for conducting investigations of unauthorized configuration changes.
126. Following the audit [REDACTED] conducted an EOC assessment and identified six configuration change management processes for High Impact BCSs which lacked detailed procedural steps. [REDACTED] was able to provide a process, complete with a process flow and decision points, which indicated any anomalous results should result in escalation to other groups and individuals to resolve. However, [REDACTED] could not provide a documented process for investigating detected unauthorized changes.
127. [REDACTED] identified the root-cause of this violation as a lack of documented steps for documenting or investigating detected unauthorized changes.
128. The violation began on July 1, 2016, when the Standard became mandatory and enforceable on the Entity because prior to Version 5 the CIP Standards and Requirements did not require entities to have a documented process for investigating unauthorized changes to baselines. The violation ended on February 28, 2018, when the Entity completed its Mitigation Plan.
129. [REDACTED] determined the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. [REDACTED] failure to have detailed work instructions could leave a responding technician unsure of what steps or actions should be taken in response to an unauthorized change, creating an opportunity for key, time sensitive steps to be omitted and resulting in an unstable or vulnerable energy management system. However, [REDACTED] had a documented process that addressed what to do during normal baseline

Attachment A

update activities and how to respond to any unexpected results. Further, [REDACTED] reviewed tickets generated from monitoring changes to the baseline configurations and did not find any instances of unauthorized changes. [REDACTED] subject matter experts would have relied on team training and job experience to address any unauthorized changes.²¹

Mitigating Actions for [REDACTED]

130. On May 23, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-010-2 R2. On June 22, 2018, [REDACTED] accepted the Mitigation Plan.
131. To mitigate this violation, the Entity:
 - i. performed an EOC analysis and identified all procedures for High Impact BCS that require enhancements to include the process for documenting and investigating detected unauthorized changes;
 - ii. developed narrative for enhancements by scripting the specific steps to be performed by subject matter experts when baseline inconsistencies are observed;
 - iii. incorporated the enhancements, including the creation of new controls, into the CIP-010 procedures for High Impact BCS. Established links to other relevant cyber security policies and procedures;
 - iv. obtained and documented the required approvals and sign-offs of revised documentation before training;
 - v. provided training to individuals who perform the tasks covered by the procedures. Designed the training to sustain ongoing content updates, tracking and delivery;
 - vi. communicated and disseminated documentation enterprise-wide by notifying impacted personnel of updates to documentation, posting new documentation on [REDACTED] and retiring previous versions; and
 - vii. corrected deficiencies found while completing the previous milestones. Utilizing all new or updated policies, procedures, work instructions and/or training, mitigated for any deficiencies identified during the completion of previous milestones. Identified any changes to BCS assets from the initial 1st Quarter 2017 CIP-002 BCS lists, and where necessary, mitigated per new updated policies, procedures, work instructions and/or training.
132. On May 29, 2018, the Entity certified to [REDACTED] that it completed the Mitigation Plan as of February 28, 2018. On August 21, 2018, [REDACTED] verified the Entity completed the Mitigation Plan by February 28, 2018.

I. CIP-011-2 R1, Part 1.2 ([REDACTED])

²¹ According to the CIP-010-2 Table of Compliance Elements, this noncompliance warranted a “Medium” VRF and a “Severe” VSL.

Attachment A

133. CIP-011-2 helps to prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

134. CIP-011-2 R1, Part 1.2 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-011-2 Table R1– Information Protection.

P1.2. Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.

[CEII] *Description of Violation and Risk Assessment for* [REDACTED]

135. During a FERC-led Compliance Audit conducted from [REDACTED] [REDACTED] FERC determined that the Entity, as a [REDACTED] was in violation of CIP-011-2 R1. [REDACTED] did not identify a SAN, used to store security configurations of its BCAs, as a BCSI repository. [REDACTED] later determined the Entity was specifically in violation of CIP-011-2 R1, Part 1.2.

136. The FERC audit team found that since the SAN stored baseline and security configurations, [REDACTED] should have categorized the SAN as a BCSI storage location. [REDACTED]
[REDACTED]
[REDACTED]

137. [REDACTED] conducted an extent of condition assessment and did not find any additional BCSI storage locations not already identified and verified.

138. [REDACTED] identified the root-cause of this violation as a lack of documented methodology that included a detailed assessment to account for all locations that may contain BCSI.

139. The violation began on July 1, 2016, when [REDACTED] commissioned the SAN without implementing procedures to protect the stored BCSI, and ended on April 25, 2018, when the Entity completed its Mitigation Plan.

140. [REDACTED] determined the violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. [REDACTED] failure to identify and protect BCSI associated with BCAs could have permitted critical information to be stored on more easily accessible and less protected systems, leaving it vulnerable and more susceptible to individuals with malicious intent. However, the overlooked server was within a secured cabinet that had card reader controlled access, which was located within a partitioned section of the ESP. Only five individuals had access to the cabinet where the SAN was located, and all were screened and trained, and had authorized access based on need. Access to

Attachment A

the security configurations identified as BCSI stored on the SAN was limited to individuals with authorized access to the tool used to retrieve such information. Further, the storage backup, although not classified as a BCSI, was protected at the same level as a BCA which exceeded the level of security required for BCSI.²²

Mitigating Actions for [REDACTED]

141. On May 23, 2018, the Entity submitted a Mitigation Plan to [REDACTED] addressing the violation of CIP-011-2 R1, Part 1.2. On June 22, 2018, [REDACTED] accepted the Mitigation Plan.
142. To mitigate this violation, the Entity:
 - i. for the cited BCSI storage location, determined and documented that a related access role existed in the [REDACTED]
 - ii. performed an EOC analysis to identify any BCSI storage locations that had not been properly identified and found none;
 - iii. performed root cause analysis for the storage location not being properly identified;
 - iv. developed a list of countermeasures leveraging results from the root cause analysis. Developed additional countermeasures by comparing NERC's "Security Guideline for the Electricity Sector: Protecting Sensitive Information" to the existing documentation comprising the information protection program (IPP);
 - v. addressed any EOC findings by: (1) creating any necessary additional [REDACTED] access roles for any BCSI Storage Location(s) identified; (2) assigning access to any new storage locations identified; and (3) properly classifying and labeling the electronic and/or physical documents for any new storage locations identified;
 - vi. implemented countermeasures for enterprise-wide methodology to identify BCSI. Created and/or revised processes documentation to ensure there is an explicit methodology for identifying existing and new electronic and/or physical BCSI;
 - vii. updated and delivered training on the methodology for identifying, labeling, transmitting, and storing of BCSI and its storage locations as per the documentation updates made to the IPP. Scheduled and administered training for all users across all business units with access to approved BCSI storage locations. (Note: Procedures indicate that IPP training is to be repeated annually and is also to be provided for new personnel that will be having access to BCSI and/or any BCSI storage locations.); and

²² According to the CIP-011-2 Table of Compliance Elements, this noncompliance warranted a "Medium" VRF and a "Severe" VSL.

Attachment A

- viii. communicated and disseminated newly revised IPP documentation enterprise-wide by notifying impacted personnel of the documentation updates and posting all new, revised documentation on [REDACTED] and retiring all related previous documents.
143. On August 8, 2018, the Entity certified to [REDACTED] that it completed the Mitigation Plan as of April 25, 2018. [REDACTED] will verify the Entity's completion of the mitigating actions.

Attachment 2

FERC Final Audit Report dated [REDACTED]

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.



Final Audit Report

Docket No. PA16-7-000

NERC ID# [REDACTED]

Date of Report: [REDACTED]

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

Table of Contents

I. Executive Summary	4
Overview	4
[REDACTED]	5
[REDACTED]	6
II. Audit Process	7
Objectives	7
Scope and Methodology	7
Confidentiality	8
Critical Energy/Electric Infrastructure Information (CEII)	8
Audit Participants.....	9
III. Audit Findings and Recommendations	10
Possible Violations.....	10
CIP-004-6, Requirement R3 - Personnel Risk Assessment Program .	10
CIP-004-6, Requirement R4 - Access Management Program.....	11
CIP-005-5, Requirement R1 - Electronic Security Perimeter	12
CIP-006-6, Requirement R1 - Physical Security Plan.....	13
CIP-006-6, Requirement R2 - Visitor Control Program.....	14
CIP-007-6, Requirement R1 - Ports and Services	15
CIP-007-6, Requirement R2 - Security Patch Management.....	16
CIP-007-6, Requirement R3 - Malicious Code Prevention	18
CIP-007-6, Requirement R4 - Security Event Monitoring	19
CIP-007-6, Requirement R5 - System Access Control	20
CIP-010-2, Requirement R2 - Configuration Monitoring	22
CIP-011-2, Requirement R1 - Information Protection	23
Other Risk(s) Identified	24
CIP Reliability Standards Documentation.....	24
Staff Training of CIP Reliability Processes and Procedures	26

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

CIP-002-5.1, Requirement R1 - Identification and Categorization of BES Cyber System.....	27
CIP-004-6, Requirement R4 - Access Management Program.....	28
CIP-005-5, Requirement R1 - Electronic Security Perimeter	28
CIP-005-5, Requirement R1 - Electronic Security Perimeter	29
CIP-007-6, Requirement R1 - Ports and Services	29
CIP-007-6, Requirement R3.1 - Malicious Code Prevention	30
CIP-007-6, Requirement R4 - Security Event Monitoring	31
CIP-007-6, Requirement R5 - System Access Control	32
CIP-010-2, Requirement R1 - Configuration Change Management ..	32
CIP-010-2, Requirement R1 - Configuration Change Management ..	33
CIP-010-2, Requirement R2 - Configuration Monitoring	34
CIP-010-2, Requirement R3 - Vulnerability Assessments	34
CIP-011-2, Requirement R1.1 - Information Protection	35
CIP-011-2, Requirement R1.2 - Information Protection	35
CIP-002-5.1, Requirement R1 - Identification and Categorization of BES Cyber System.....	35
CIP-002-5.1, Requirement R1 - Attachment 1 Criteria 1.4 Identification and Categorization of BES Cyber System	37
IV. Post-Audit Activities.....	38

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

I. Executive Summary

Overview

The Division of Reliability Standards and Security (DRSS) in the Office of Electric Reliability of the Federal Energy Regulatory Commission (FERC, or the Commission) conducted a non-public audit of [REDACTED] ([REDACTED]¹ [REDACTED] is a Registered Entity with the North American Electric Reliability Corporation (NERC). The audit evaluated [REDACTED] compliance with the applicable mandatory Reliability Standards for the Bulk-Power System Critical Infrastructure Protection (CIP) Reliability Standards (CIP Reliability Standards).² [REDACTED]

Staff from [REDACTED], [REDACTED], and [REDACTED] participated in the audit, including the on-site portion, and had access to the audit evidence. The audit was commenced on [REDACTED] and covered the period of [REDACTED].

¹ [REDACTED]

² 18 C.F.R. Part 40 (2016).

³ [REDACTED]

⁴ [REDACTED]

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

Audit staff identified twelve (12) Possible Violations of the CIP Reliability Standards for [REDACTED]. In addition, audit staff identified eighteen (18) other risks, each with audit staff's recommended steps to address these other risks.

Other Risks Identified (ORIs) are areas of concern and associated cybersecurity practice recommendations that audit staff identified during the audit that were not possible violations. The Commission has explained that an area of concern is a "situation that does not appear to involve a current or ongoing violation of a Reliability Standard requirement, but instead represents an area of concern that could become a violation."⁵ The cyber security practice recommendations that audit staff makes in this report are improvements to the cyber security posture of the entity that address areas that are outside the scope of the CIP Reliability Standards.

These audit results are further explained in Section III - Audit Findings and Recommendations. The Possible Violations will be processed through [REDACTED], [REDACTED], and [REDACTED] in accordance with NERC's Rules of Procedure (ROP). The audit staff recommendations associated with the ORIs will be processed by DRSS pursuant to its audit implementation procedures, as discussed below in Section IV - Post-Audit Activities of this report.

[REDACTED]

⁵ *Compliance with Mandatory Reliability Standards*, 126 FERC ¶ 61,038 P 13 (2009).

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

[REDACTED]

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

II. Audit Process

Objectives

The audit evaluated [REDACTED] compliance with the CIP Reliability Standards that are applicable to its registered and functional responsibilities identified above.

[REDACTED]

Scope and Methodology

The audit was commenced on [REDACTED] and covered the period of [REDACTED]. The audit evaluated compliance with the CIP Reliability Standards as follows:

- CIP Reliability Standards version 5⁸ (CIP v5) for the period of [REDACTED], and;
- CIP Reliability Standards version 3⁹ (CIP v3), for the period of [REDACTED] (the end date of the last [REDACTED] CIP compliance audit) through [REDACTED] (the end effective date of CIP v3).

7

[REDACTED]

⁸ *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 81 Fed. Reg. 4,177 (Jan 26, 2016), 154 FERC ¶ 61,037 (2016), *reh'g denied*, 156 FERC ¶ 61,052 (2016); *see* Reliability Standards: CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2. *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 FR 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, 46 FERC ¶ 61,188 (2014); *see* Reliability Standards: CIP-002-5.1a, CIP-005-5, and CIP-008-5.

⁹ *North American Electric Reliability Corp.*, 128 FERC ¶ 61,291, *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009), *order on compliance*, 130 FERC ¶ 61,271 (2010); *see* Reliability Standards: CIP-002-3, CIP-003-3, CIP-004-3, CIP-005-3, CIP-006-3, CIP-007-3, CIP-008-3, and CIP-009-3.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

Audit fieldwork primarily consisted of evidence requests and reviews, teleconferences, and Subject Matter Expert (SME) interviews. Audit staff issued data requests to gather evidential information pertaining to the [REDACTED] CIP activities and operations. Audit staff conducted teleconferences to discuss the audit scope and objectives, data requests and responses, technical and administrative matters, and compliance concerns. Audit staff conducted a site visit during the week of [REDACTED] to interview SMEs, observe operating practices, processes and procedures of staff and equipment, and further understand the [REDACTED] functions, operations, practices, and regulatory and corporate compliance programs. While on site, audit staff interviewed employees and managers responsible for performing tasks within the audit scope and analyzed documentation to verify compliance with requirements. Additionally, audit staff conducted several field inspections and observed the functioning of certain assets identified by [REDACTED] as High, Medium, or Low Impact. Audit staff also interviewed compliance program managers and staff, and employees responsible for day-to-day compliance and regulatory oversight activities.

The audit staff evaluated the data, information, and evidence provided by [REDACTED] for sufficiency, appropriateness, and validity. Documentation submitted in the form of policies, procedures, e-mails, logs, studies, data sheets, etc., was validated, substantiated, and crosschecked for accuracy as appropriate. Requirements that required a sampling to be conducted were developed based on the significance of the sampling to the reliability of the Bulk Electric System (BES).

Confidentiality

Confidentiality of all evidence received is governed under 18 CFR Part 388 (2016) (Information and Requests).

Critical Energy/Electric Infrastructure Information (CEII)

The audit report contains Critical Energy/Electric Infrastructure Information (CEII) pursuant to 18 C.F.R. § 388.113 (2016). The recipients (except for employees of the owner-operator, [REDACTED] of this document are required to execute a non-disclosure agreement (NDA) prior to receipt certifying that access to CEII is provided pursuant to the terms and restrictions of the NDA.¹⁰

The specific paragraphs that are categorized as CEII are designated as such.

¹⁰ See: Critical Energy/Electric Infrastructure Information General Non-Disclosure Agreement, <https://www.ferc.gov/legal/ceii-foia/ceii/gen-nda.pdf>.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

Audit Participants

The audit was conducted by DRSS with the assistance of the Division of Audits and Accounting in the Commission's Office of Enforcement. [REDACTED], and [REDACTED] participated during the audit, including the on-site portion, and had access to the audit evidence.

Document must be treated as CEII until the CEII Coordinator removes the designation.

CIP-004-6, Requirement R4 - Access Management Program

██████ did not properly track access authorizations of its domain administrator accounts. In addition, ██████ did not have sufficient controls over the distribution of physical keys, which led to the improper provisioning of physical keys to employees without authorization. As a result, ██████ was not in compliance with the CIP Reliability Standard CIP-004-6 Requirement R4. ██████

CIP-004-6 R4 requires that each Responsible Entity implement one or more documented access management program(s) that (R4.1) have a process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: (R4.1.1) Electronic access, (R4.1.2) Unescorted physical access into a Physical Security Perimeter; (R4.1.3) access to designated storage locations, whether physical or electronic, for BES Cyber System Information; and (R4.2) verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.¹²

As part of its access management program, [REDACTED] implemented procedures intended to control electronic access to its BES Cyber System Information (BCSI). The audit team analyzed [REDACTED] access management policies and procedures, evaluated access records, and observed employee access practices. The audit team discovered that [REDACTED] did not effectively track access authorizations or review access to its domain administrator accounts within its [REDACTED]

¹² CIP-004-6 at 15-19.

11

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

[REDACTED] [REDACTED] acknowledged this deficiency in response to an audit staff data request.¹⁴

Additionally, the audit team discovered that [REDACTED] [REDACTED] who was tasked with distributing physical keys that provide employees and contractors unescorted access to identified BES Cyber System assets did not have authorized unescorted access to the BES Cyber System assets despite having physical copies of all the keys for [REDACTED] Medium Impact substations.¹⁵ In another instance, a key was issued to someone who did not have authorized unescorted physical access according to [REDACTED] access list.¹⁶ Finally, the audit staff observed two instances during its site visit in which [REDACTED] could not locate keys provisioned for access to a door.

CIP-005-5, Requirement R1 - Electronic Security Perimeter

[CEII]

[REDACTED]

Pertinent Guidance

CIP-005-5 R1.3 requires Electronic Access Points for both High and Medium Impact BES Cyber Systems to require access permissions for all inbound and outbound communication, including the reason for granting access, and deny all other access by default.

Background

[REDACTED] used Internet Control Message Protocol (ICMP), a supporting protocol in the Internet protocol suite on its network devices for error messages and operational information. ICMP is encapsulated within Internet Protocol (IP), similar to how Transmission Control Protocol (TCP) is encapsulated. TCP encapsulated within IP is known as TCP/IP. It is common industry practice for

¹⁴ See evidence artifacts: (1) CIP-004-R4-L13-05_Evidence-CEII.pdf and (2) CIP-004-R4-L13-05_Cover_Letter-CEII submitted August 29, 2016.

¹⁵ See evidence artifact: CIP-004-R4-L13-05_Evidence-CEII.pdf.

¹⁶ See evidence artifact: of SV-L3-CIP-006-04_Evidence-CEII.pdf at 3.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

network engineers or system administrators to block the echo component of ICMP for sensitive or critical networks.

[CEII]



CIP-05-005 R1.3 states that access permission must be granted for all inbound and outbound communication to High and Medium Impact BES Cyber Systems, and a reason must be provided when access is granted. [REDACTED] allowed such communication access to its BES Cyber Systems without maintaining required documentation to support the reason it granted the access.

CIP-006-6, Requirement R1 - Physical Security Plan

[CEII]



Pertinent Guidance

CIP-006-6 R1.3 requires Responsible Entities to implement one or more documented physical security plan(s) that, where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted

¹⁷ A demilitarized zone (DMZ) is a physical or logical sub-network that contains an organization's external-facing services to an untrusted network, usually the Internet.

¹⁸ Per NERC's Glossary of Terms, the PSP is a physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.

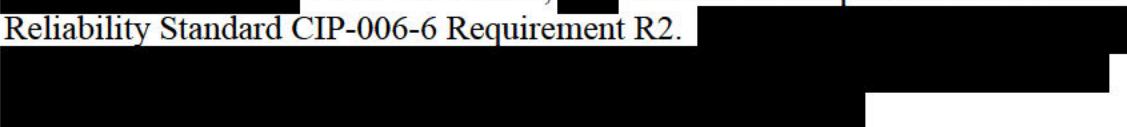
Background

[CEII]



CIP-006-6, Requirement R2 - Visitor Control Program

did not properly maintain complete visitor access control logs for its PSP. As a result, was not in compliance with the CIP Reliability Standard CIP-006-6 Requirement R2.



Pertinent Guidance

CIP-006-6 R2 requires Responsible Entities to implement one or more documented visitor control program(s) that require: (2.1) 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; (2.2) 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; and (2.3) retention of visitor logs for at least ninety calendar days.

Background

¹⁹ See evidence artifact: CIP-006-R1-L2-08_Evidence-CEII.pdf, page 13.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

Background

Audit staff reviewed [REDACTED] documents pertaining to logical network accessible ports associated with BES Cyber Assets to determine whether the company implemented appropriate processes and procedures for enabling, disabling, or restricting the ports. Audit staff found that [REDACTED] maintained records that listed open ports and services at its BES Cyber Assets. However, [REDACTED] did not provide documentation that supported process and procedures the company implemented to establish that there was a need for the open ports. Based on the record, the audit team could not determine that [REDACTED] performed an analysis to evaluate whether there was a need for the ports to remain open. [REDACTED] explained that its [REDACTED] business unit preliminarily updated the lists prior to the audit. Moreover, [REDACTED] maintained that the list was not complete, and that the [REDACTED] business unit was waiting on confirmation from a vendor to update the remaining ports and services descriptions to become compliant with the CIP Reliability Standard requirements.²³

[CEII]



CIP-007-6, Requirement R2 - Security Patch Management

[REDACTED] documented processes of cyber security patch management for its BES Cyber Assets did not include procedures for evaluating the applicability of new security packages prior to installation that were consistent with the standard requirements. Specifically, [REDACTED] process neither appropriately assessed the applicability of new security patches for Cyber Assets nor provided for the

²³ See evidence artifact: CIP-007-R1-L11-04_Evidence-CEII.pdf.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

retention of tracking records that support the performance of tests of patches. As a result, [REDACTED] was not in compliance with the CIP Reliability Standard CIP-007-6 Requirement R2. [REDACTED]

[REDACTED]

Pertinent Guidance

CIP-007-6 R2 requires Responsible Entities to implement one or more documented process(es) that (2.1) have a patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets; (2.2) at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation; (2.3) within 35 calendar days of the evaluation completion, take one of the following actions: (a) apply the applicable patches, (b) create a dated mitigation plan, or (c) revise an existing mitigation plan; and (2.4) implement any mitigation plans.

Background

[CEII] [REDACTED]

[CEII] [REDACTED]

²⁴ See evidence artifact: CIP-007-R2-L1-01_Evidence-CEII at 27.

²⁵ See evidence artifact: CIP-007-R2-L1-01_Evidence-CEII at 6, section 5.2.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

with its documented operating processes. Moreover, [REDACTED] did not provide documentation to support its past performance of tests of patches on test machines prior to deployment in the production environment.

[CEII] CIP-007-6 R2 requires [REDACTED] to implement a process to track, evaluate, and install new security patches for applicable Cyber Assets. [REDACTED] did not test its patches prior to uploading them in the production environment. Consequently, the company did not appropriately assess the applicability of new security patches for Cyber Assets. Furthermore, [REDACTED] did not maintain records on the results of tests of cyber security patches it installed. As a result of the lack of records, [REDACTED] was unable to provide evidence to prove compliance with the tracking requirement of the standard.

CIP-007-6, Requirement R3 - Malicious Code Prevention

[CEII] [REDACTED]

Pertinent Guidance

CIP-007-6 R3 requires Responsible Entities to implement one or more documented process(es) that (3.1) deploy method(s) to deter, detect, or prevent malicious code; (3.2) mitigate the threat of detected malicious code; and (3.3) for those methods that use signatures or patterns, have a process for the update of the signatures or patterns for High or Medium Impact BES Cyber Systems and their associated (1) Electronic Access Control or Monitoring Systems (EACMS), (2) Physical Access Control Systems (PACS), and Protected Cyber Assets (PCA).

Background

[CEII] [REDACTED]

[REDACTED]

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

[REDACTED]

[CEII] [REDACTED]

[CEII] [REDACTED]

CIP-007-6, Requirement R4 - Security Event Monitoring

[CEII] [REDACTED]

[REDACTED]

²⁸ Intrusion Prevention Systems and Intrusion Detection Systems are devices or software applications that monitor and protect a network.

²⁹ Electronic Security Perimeter is a CIP Reliability Standards and NERC Glossary defined term for the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

³⁰ See evidence artifact: Attachment A – CIP Version 5 Evidence Request [REDACTED] 6.22.16.xlsx.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

[REDACTED]

Pertinent Guidance

CIP-007-6 R4.1 requires Responsible Entities to 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 include, as a minimum, each of the following types of events: (R 4.1.1) detected successful login attempts; (R 4.1.2) detected failed access attempts and failed login attempts; and (R 4.1.3) detected malicious code.

Background

[CEII] [REDACTED]

CIP-007-6, Requirement R5 - System Access Control

[REDACTED] did not properly identify individuals who had authorized access to shared accounts. In addition, [REDACTED] did not file a TFE for its [REDACTED] device, nor demonstrate its implementation of compensating and/or mitigating measures on the [REDACTED] device(s). As a result, [REDACTED] was [REDACTED]

[REDACTED]

Pertinent Guidance

CIP-007-6 R5 requires each Responsible Entity to implement one or more documented process(es) that have (R5.1) method(s) to enforce authentication of interactive user access, where technically feasible; (R5.2) 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); (R5.3) identify individuals who have authorized access to shared accounts; and (R5.7) where technically

³¹ *Id.*

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

provided supporting documents to audit staff that indicated that [REDACTED] was planning to fix the issue.³⁶

During the site visit, [REDACTED] demonstrated the authentication and login for its [REDACTED] device through an intermediate system. [REDACTED] stated that the device only supported a single username and password that must be shared with the different operators, and the [REDACTED] device does not support alerts for unsuccessful attempts or have a lock out feature.

Although the [REDACTED] device did not meet the requirement of CIP-007-6 Requirement R5 Part 5.7, per NERC's Rules of Procedure (ROP), [REDACTED] was required to use compensating and/or mitigating measures that achieve at least a comparable level of security for the Bulk Electric System as would strict compliance with the applicable requirement.³⁷ Furthermore, [REDACTED] was required to file a TFE with [REDACTED] or NERC that described the covered asset and the mitigating measures.³⁸ Audit staff discovered that [REDACTED] did not file a TFE for Requirement R5 Part 5.7, thus no mitigating measures were described, as required.

CIP-010-2, Requirement R2 - Configuration Monitoring

[REDACTED] did not have documented processes for investigating detected unauthorized changes to baseline configurations of its BES Cyber Assets, as required. As a result, [REDACTED] was not in compliance with the CIP Reliability Standard CIP-010-2 Requirement R2. [REDACTED]

Pertinent Guidance

CIP-010-2 R2 requires Responsible Entities to implement one or more documented process(es) that monitor at least once every 35 calendar days for changes to the baseline configurations, and then document and investigate detected unauthorized changes.

Background

³⁶ See evidence artifact: CIP-004-R4-L13-05_Evidence-CEII.pdf.

³⁷ Appendix 4D to the Rules of Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards, at 5-6. (Apr. 1, 2016) and at 3 (July 1, 2016).

³⁸ *Id.* at 6 (Apr. 1, 2016) and 3 (July 1, 2016).

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

[CEII]



CIP-011-2, Requirement R1 - Information Protection

█ did not properly identify a storage area network used to store security configurations of its BES Cyber Assets as a BCSI Storage Location. As a result, █ was not in compliance with the CIP Reliability Standard CIP-011-2 Requirement R1. █

Pertinent Guidance

CIP-011-2 R1 requires the Responsible Entity to implement one or more documented information protection program(s) that has (R1.1) method(s) to identify information that meets the definition of BCSI; and (R1.2) procedure(s) for protecting and securely handling BCSI, including storage, transit, and use.

Background

[CEII]



³⁹ See evidence artifact: CIP-010-R2-L1-01_Evidence-CEII.pdf at 5.

⁴⁰ See evidence artifact: IM-CIP-010-EVD-Any_Unauth_Changes-CEII.pdf.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.



Other Risk(s) Identified

CIP Reliability Standards Documentation

Audit staff's review of documentation used to demonstrate compliance with the CIP Reliability Standards identified numerous areas of concern that did not appear to involve current or ongoing violations of Reliability Standard requirements. However, these areas of concern represent risks that could lead to significant deficiencies in the cyber security program that could become violations. These concerns present both security and compliance risks.

Examples include, but are not limited to, the following:

1. In [REDACTED] BCS identification tool, audit staff found the evidence provided did not match [REDACTED] documented instructional process in two instances: (1) the [REDACTED] process document referenced data fields that the corresponding spreadsheets did not have;⁴¹ and (2) [REDACTED] BCS categorization tool was not fully completed for approximately ten percent of the assets evaluated.⁴² [REDACTED] provided corrected updates in a subsequent data request.⁴³
2. [REDACTED] used affirmations as evidence of compliance where more substantive evidence could be used that would not be overly burdensome.⁴⁴
3. [REDACTED] lacked approval dates with signatures on some approval documents.

⁴¹ See evidence artifacts: (1) CIP-002-R1-L1-01 [REDACTED]-CIP-002-INS-BCS_Categorization-CEII.pdf and (2) CIP-002-R1-L1-03 [REDACTED]-CIP-002-EVD-BCS_List [REDACTED]-CEII.xlsm.

⁴² See evidence artifact: CIP-002-R1-L1-03 [REDACTED]-CIP-002-EVD-BES_Asset_Class [REDACTED]-CEII.xlsm.

⁴³ See evidence artifacts: (1) CIP-002-R1-L10-02_Narrative-CEII.pdf and (2) CIP-002-R1-L10-03_Narrative-CEII.pdf.

⁴⁴ See evidence artifact: CIP-002-R2-L1-01_Evidence-CEII.pdf.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

4. Several of [REDACTED] PSP drawings were inaccurate or lacking in detail. [REDACTED]
- [REDACTED]
- [REDACTED] Finally, there was a drawing of a PSP, but only half of the PSP was shaded correctly in the drawing.⁴⁸
5. The assets listed within [REDACTED] documentation did not sufficiently correlate to the assets listed in response to audit staff's data request Attachment A Spreadsheet.⁴⁹ Different names of assets were used in various [REDACTED] documents, which differed from the names provided in response to the Attachment A Spreadsheet. In addition, [REDACTED] listed different vendors for the same equipment, with various documents listing one vendor and not the other.⁵⁰
6. The documentation [REDACTED] provided supporting the exercise of its Cyber Security Incident Response Plan did not clearly demonstrate compliance. Specifically, audit staff is concerned that [REDACTED] does not appear to have followed its documented process for reporting "events" to the on-call information security analyst.⁵¹

⁴⁵ See evidence artifact: CIP-006-R1-L2-04_Evidence-CEII.pdf at 10.

⁴⁶ See evidence artifact: CIP-006-R1-L2-05_Evidence-CEII.pdf at 16.

⁴⁷ See evidence artifacts: (1) CIP-006-R1-L2-05_Evidence-CEII.pdf, drawing on page 18 of and (2) PACL.20160603 [REDACTED].NO515.csv.

⁴⁸ See evidence artifact: CIP-006-R1-L2-08_Evidence-CEII.pdf, Room 3410 at 6.

⁴⁹ See evidence artifact: CIP-007-R1-L2-01_Evidence-CEII.

⁵⁰ For example, see page 9 of CIP-007-R1-L2-01_Evidence-CEII. [REDACTED] lists five assets as [REDACTED], but within the corresponding Attachment A spreadsheet [REDACTED] lists one asset as [REDACTED] router for [REDACTED] three as [REDACTED], and one as [REDACTED]

⁵¹ See evidence artifact: CIP-008-R2-L1-01_Evidence-CEII.pdf.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

7. While [REDACTED] had sufficient criteria and processes for evaluating possible criminal history when PRAs have adverse findings, [REDACTED] did not sufficiently document these criteria and processes in various instances.⁵²
8. Various [REDACTED] documents had minor mistakes in them, however misuse of terms was common through all of the CIP Reliability compliance documents. For example, [REDACTED] documents referred to “deploying malicious code tools” instead of “deploying malicious code detection tools.”⁵³ Another example of inaccuracies was referencing to assets that are no longer in service.⁵⁴
9. [REDACTED]

Recommendation 1

Conduct a thorough review of CIP Reliability Standards compliance documentation, identify areas of improvement to include but not be limited to instances where the documented instructional processes are inconsistent with actual processes employed or where inconsistencies exist between documents, and modify documentation and processes accordingly.

Staff Training of CIP Reliability Processes and Procedures

During fieldwork, audit staff identified various instances in which [REDACTED] staff was not familiar with relevant details of various cyber security processes and procedures in place, yet presented them to demonstrate compliance with the CIP Reliability Standards. Examples include, but are not limited to, the following:

1. [REDACTED] staff did not have knowledge of how the vendor [REDACTED] contracted to perform background checks for [REDACTED] employees was sufficiently

⁵² See evidence artifacts: (1) CIP-004-R3-L11-04_Evidence-CEII.pdf; (2) CIP-004-R3-L11-05_Evidence-CEII.pdf; (3) CIP-004-R3-L13-03_Evidence-CEII.pdf; (4) CIP-004-R3-L13-02_Evidence-CEII.pdf; and (5) SV-L7-CIP-004-01_Evidence_09.16.16.

⁵³ See evidence artifact: CIP-007-R3-L2-01_Evidence-CEII.pdf.

⁵⁴ See evidence artifacts: (1) SV-LV6-CIP-007-03_Narrative-CEII and CIP-007-R4-L13-08_Evidence-CEII, both specific to [REDACTED] devices.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

meeting CIP standard requirements for background checks pursuant to CIP-004-6 R3.4.⁵⁵

2. When providing the list of key custodians in response to audit staff's data request, [REDACTED] staff identified a key custodian for a [REDACTED] [REDACTED] who had not been identified in any previous documentation.⁵⁶ During the site visit, [REDACTED] staff stated that the [REDACTED] was under deactivation, but they were uncertain whether it had been deactivated yet. In response to an onsite data request about this data center, [REDACTED] stated that it was still in the process of being deactivated and the network devices remaining have no production data running through the segment.⁵⁷

3. [REDACTED]

Recommendation 2

Upon completion of recommendation #1, develop a comprehensive staff training program for those processes and provide training to all relevant [REDACTED] staff and contractors.

CIP-002-5.1, Requirement R1 - Identification and Categorization of BES Cyber System

[REDACTED] implemented a rule on the firewall at [REDACTED] in [REDACTED] with the designation of "temporary." During fieldwork, audit staff discovered the rule remained with the designation of "temporary" nearly five years later.⁵⁹

Recommendation 3

⁵⁵ [REDACTED] is a private company that offers fraud deterrent/detection services and investigative and security consulting services.

⁵⁶ See evidence artifact: SV-L3-CIP-006-01_Evidence-CEII.pdf.

⁵⁷ See evidence artifact: SV-L7-CIP-006-02_Narrative-CEII.pdf.

⁵⁸ See evidence artifact: CIP-008-R1-L15-02_Evidence-CEII.pdf.

⁵⁹ See evidence artifacts: (1) Pmr rulebase.pdf; (2) IM-CIP-005-EVD-PRM_Change_Ticket_71722-CEII.pdf; (3) IM-CIP-005-EVD-PMR-CFW-09132016_Logs-CEII.xls; and (4) IM-CIP-005-EVD-PMR-CRW-09142016_Logs-CEII.xls.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

Modify firewall policies and procedures to define the term ‘temporary’ to include parameters around the use of the “temporary” designation, e.g., review temporary designations within a specific timeframe.

CIP-004-6, Requirement R4 - Access Management Program

The process used by [REDACTED] to import revocations of access from its SAP HR system to its access management system presents the risk that access may be revoked greater than 24 hours after the termination action, e.g. termination or retirement, was initiated.⁶⁰ There is a potential gap in time between approval of a request for termination action entered into the SAP HR system and the time the request is approved in [REDACTED] access management system that may be greater than the 24 hours that CIP-004-6 R5.1 allows.

Recommendation 4

Modify [REDACTED] access management program to start the revocation 24 hours from the moment the revocation is entered into the SAP HR system, and not when the revocation request is transferred to the [REDACTED] access management system.

CIP-005-5, Requirement R1 - Electronic Security Perimeter

[REDACTED] practices for conducting Interactive Remote Access (IRA, or “IRA CA”) allow for other network communications to be made during an IRA session. Although no CIP Reliability Standard requirement directly limits other network communications on a Cyber Asset that is conducting IRA, audit staff recommends that all Cyber Assets that are conducting IRA have all other network access disabled other than to the BES Cyber System they are remotely accessing, unless for a documented business or operational need. Disabling other network access would include disabling split tunneling if the IRA CA is using Virtual Private Network (VPN) to connect to the Intermediate System, disabling dual-homing if the IRA CA has more than one network connection, or disallowing general internet access to minimize the overall attack surface and risk to [REDACTED] cyber security posture.

Recommendation 5

Modify its CIP reliability process documents to disable all other network access for clients of IRA, unless for a documented business or operational need.

⁶⁰ See evidence artifact: CIP-004-R5-L2-01_Evidence-CEII.pdf.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

CIP-005-5, Requirement R1 - Electronic Security Perimeter

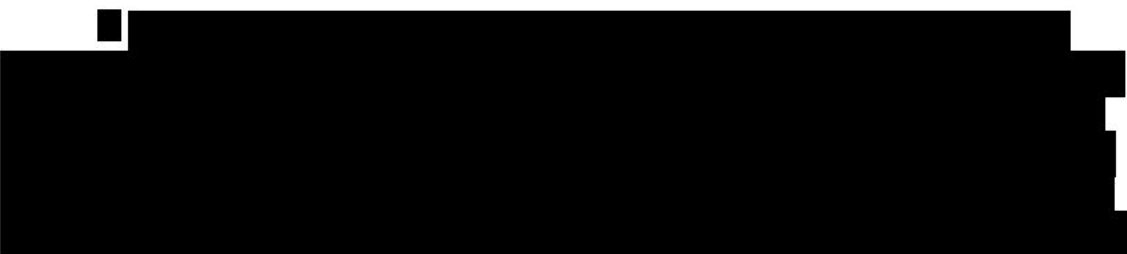
[CEII]



Recommendation 6

Evaluate whether the current thresholds that are used to initiate an investigation are appropriate based on risk. If the evaluation determines that those thresholds are not appropriate, modify the threshold based on that evaluation, and modify the CIP reliability process documents, as appropriate.

CIP-007-6, Requirement R1 - Ports and Services



⁶³ See evidence artifact: CIP-005-R1-L14-03_Evidence_CEII Step 1.1.1 at 12.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

[REDACTED]

Recommendation 7

Evaluate the use of the full range of ephemeral ports, and based on the evaluation, limit the range of ports that are open, as appropriate, ensuring that the limit would not affect normal and/or emergency operations.

CIP-007-6, Requirement R3.1 - Malicious Code Prevention

[CEII] [REDACTED]

⁶⁴ An ephemeral port is a short-lived transport protocol port for Internet Protocol (IP) communications allocated automatically from a predefined range by the IP stack software. An ephemeral port is typically used as the port assignment for the client end of a client–server communication to a well-known port on a server.

⁶⁵ [REDACTED]

⁶⁶ See evidence artifact: CIP-007-R3-L2-01_Evidence-Supplemental at 4.

⁶⁷ [REDACTED]

⁶⁸ [REDACTED]

⁶⁹ See evidence artifact: CIP-007-R3-L2-01_Evidence-Supplemental at 3.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

[REDACTED]

Recommendation 8

[CEII] [REDACTED]

CIP-007-6, Requirement R4 - Security Event Monitoring

[REDACTED]

Recommendation 9

[REDACTED]

⁷¹ See evidence artifact: CIP-007-R3-L12-05_Evidence-CEII at 1.

⁷² *Id.*

⁷³ See evidence artifacts: (1) CIP-007-R4-L13-03_Narrative-CEII and (2) CIP-007-R4-L1-01_Evidence-CEII [REDACTED]

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

CIP-007-6, Requirement R5 - System Access Control

Audit staff requested the policy, procedures, and processes for limiting the number of unsuccessful authentication attempts and the threshold of unsuccessful authentication attempts for generating alerts for [REDACTED] Information Management (IM) business unit. [REDACTED] procedures covering the system access control requirements of CIP-007-6 R5.7 are governed by a document called CS-CIP-007-PRO_PACS-CEII.⁷⁴ However, audit staff discovered that the document only covers [REDACTED] PACS.⁷⁵ Audit staff noted that [REDACTED] did not have any Medium Impact assets at its Control Centers, but referenced [REDACTED], in its documentation.⁷⁶ Audit staff informed [REDACTED] that the supplied documentation did not address this requirement for these business units. [REDACTED] responded that although the system controls for limiting the number of unsuccessful authorization attempts or alerting for unsuccessful authentication are in effect, the procedure does not specifically address these control measures.⁷⁷ It is an unnecessary risk to not limit the number of unsuccessful authorization attempts.

Recommendation 10

Incorporate system controls for limiting the number of unsuccessful authorization attempts or alerting for unsuccessful authentication into its documented policies and procedures.

CIP-010-2, Requirement R1 - Configuration Change Management

Audit staff discovered that [REDACTED] policies and procedures allow its staff to connect to its BES Cyber Systems using corporate laptops that have the ability to connect to non-BES Cyber Systems outside of [REDACTED] ESP. The CIP Reliability

⁷⁴ See evidence artifact: CIP-007-R5-L1-01_Evidence-CEII.pdf at 176 – 193.

⁷⁵ CIP-007-6 R5.7 should cover all High- and Medium- Impact BES Cyber Systems and their associated (1) EACMS; (2) PACS; and (3) PCAs. PACS are Physical Access Control Systems.

⁷⁶ See evidence artifact: CIP-007-R5-L1-01_Evidence-CEII.pdf.

⁷⁷ See evidence artifact: (1) CIP-007-R5-L14-11_Evidence-CEII.pdf and (2) CIP-007-R5-L1-01_Evidence-CEII.pdf.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

Standards define the connection of such a device as a Transient Cyber Asset, which is a Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. During fieldwork, [REDACTED] explained that the connecting corporate laptops are only temporary, i.e., may be used for no more than 30 days. However, audit staff is concerned that these Transient Cyber Assets may have network connectivity outside of the ESP with non-BES Cyber Systems while connected to a BES Cyber System, increasing the potential attack surface on [REDACTED] system and presenting unnecessary risk to [REDACTED] cyber security posture.

Recommendation 11

Modify its policies and procedures over employee use of Transient Cyber Assets to ensure that all such assets do not have network connectivity outside of the ESP with non-BES Cyber Systems while connected to a BES Cyber System.

CIP-010-2, Requirement R1 - Configuration Change Management

CIP-010-2 R1.1.4 requires [REDACTED] to perform a baseline configuration of open ports and services of its BES Cyber Systems. [REDACTED] procedure for baselining details how an [REDACTED] employee should acquire a list of open ports and services for [REDACTED] BES Cyber Systems. However, [REDACTED] procedure did not specify the appropriate steps to be taken when open ports and services are discovered that do not match a previous baseline or that are specifically required by its vendor.⁷⁸ During fieldwork, [REDACTED] staff stated that their documentation is lacking and can be improved in this area. In addition, [REDACTED] documentation did not specify whether an investigation would result from a large discrepancy discovered between the old baseline and the new scan. Audit staff is concerned with the lack of detail in [REDACTED] procedures across its business units, presenting an unnecessary risk that an investigation would not be triggered if a new baseline resulting from a scan contained undocumented changes.

Recommendation 12

Reexamine its procedures to ensure discrepancies in open ports and services are investigated for instances where there is an undocumented variance between the baseline and the new scan.

⁷⁸ See evidence artifact: CIP-010-R1-L1-01_Evidence-CEII.pdf at 35.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

CIP-010-2, Requirement R2 - Configuration Monitoring



Recommendation 13

The IM business unit should modify the script to add the date which the comparison was performed within the output file so a future auditor can better assess the evidence.

CIP-010-2, Requirement R3 - Vulnerability Assessments

█████ processes and procedures for conducting cyber-vulnerability assessments (CVA) rely upon a template for each █████ business units to follow. During fieldwork, audit staff discovered that the content and implementation of the template varied among each business unit, which resulted in differing approaches to each CVA.⁸³ Audit staff believes that █████ should coordinate the performance of CVAs among business units to ensure continuity and completeness of the assessment.

Recommendation 14

⁷⁹ See evidence artifact: IM-CIP-010-EVD-Baseline-█████-CEII.pdf.

⁸⁰ *Ibid.*

⁸¹ *Ibid.*

⁸² *Ibid.*

⁸³ See evidence artifact: CIP-010-R3-L1-01_Evidence-CEII.pdf.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

Evaluate its processes and procedures for conducting CVAs, and consider enhancing such processes and procedures to increase the coordination among business units, where practicable.

CIP-011-2, Requirement R1.1 - Information Protection

██████ processes and procedures for identifying BCSI should be improved. Although ██████ had a clear description of what information should be identified as BCSI, ██████ did not have a documented process for its employees to follow and instead relied solely on employee training for proper identification. In addition, ██████ Information Protection Program fell short of including the guidance listed in the NERC CIPC document, “Security Guideline for the Electricity Sector: Protecting Sensitive Information.”⁸⁴

Recommendation 15

Enhance its documented processes and procedures for identifying BCSI, taking into consideration the NERC CIPC document, “Security Guideline for the Electricity Sector: Protecting Sensitive Information.”

CIP-011-2, Requirement R1.2 - Information Protection

██████ documented procedures for conducting its review of BCSI classification should be improved. ██████ procedures are focused on reviewing BCSI that reside within defined BCSI storage locations. ██████ explained that this procedure would partially identify documents not properly classified, but conceded it would miss documents not stored in defined BCSI storage locations.⁸⁵

Recommendation 16

Enhance its documented procedures for reviewing BCSI classification to include information that is not stored in defined BCSI storage locations.

CIP-002-5.1, Requirement R1 - Identification and Categorization of BES Cyber System

CIP-002-5.1 exists as part of a suite of CIP Reliability Standards related to cyber security that requires a minimum level of organizational, operational and procedural security controls to mitigate risk to BES Cyber Systems, and in doing

⁸⁴

[http://www.nerc.com/comm/CIPC/Protecting%20Sensitive%20Information%20Guideline%20Task1/Protecting%20Sensitive%20Information%20Guideline%20\(PSIGTF\).pdf](http://www.nerc.com/comm/CIPC/Protecting%20Sensitive%20Information%20Guideline%20Task1/Protecting%20Sensitive%20Information%20Guideline%20(PSIGTF).pdf)

⁸⁵ See evidence artifact: CIP-011-R1-L13-03_Evidence-CEII.pdf.

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

so mitigate risk to the BES. Correct implementation of CIP-002-5.1 requirements, including the initial identification and categorization of BES Cyber Systems supports the appropriate protections, as required by the other CIP Reliability Standards, against compromises that could lead to misoperation or instability in the BES.

[REDACTED]

[CEII] [REDACTED]

[CEII] [REDACTED]

86

[REDACTED]

⁸⁷ Real Power is the portion of electricity that supplies energy to the Load, where Load is an end-use device or customer that receives power from the electric system.

⁸⁸ Per CIP-002-5.1, Attachment 1, Criteria 2.1 a requirement for a Medium Impact BES Cyber System is “[f]or each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.”

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

[REDACTED]

[REDACTED]

Recommendation 17

[REDACTED]

**CIP-002-5.1, Requirement R1 - Attachment 1 Criteria 1.4
Identification and Categorization of BES Cyber System**

[CEII]

[REDACTED]

Recommendation 18

[REDACTED]

Designated Critical Energy/Electric Infrastructure Information (CEII)

CEII Designation Period: June 5, 2017 – June 4, 2022. Designation may be renewed.

Document must be treated as CEII until the CEII Coordinator removes the designation.

IV. Post-Audit Activities

The Possible Violations identified above in Section III will be referred for processing by [REDACTED], [REDACTED], and [REDACTED], as applicable, in accordance with NERC's ROP. The ORIs will be processed by audit staff. We further recommend that [REDACTED] and [REDACTED] coordinate the development and submittal of the following to audit staff for review:

1. A plan for implementing audit staff's ORI recommendations. [REDACTED] should provide this plan within 30 days after the final audit report is issued.
2. Quarterly reports describing progress in completing each corrective action recommended in the final audit report. [REDACTED] should make these nonpublic quarterly filings no later than 30 days after the end of each calendar quarter, beginning with the first quarter after submission of the implementation plan, and continuing until all recommended corrective actions are completed.
3. Copies of any written policies and procedures developed in response to the recommendations in the final audit report. These documents should be submitted for review in the first quarterly filing after the products are completed.