

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 [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] determination and findings of the violations of the CIP Reliability Standards listed below.

According to the Settlement Agreement, The Entity neither admits nor denies the violations, but has agreed to the assessed penalty of one million dollars (\$1,000,000), in addition to other remedies and

¹ Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards (Order No. 672), 114 FERC ¶ 61, 104 (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**

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 Notice of Penalty
The Entity
May 30, 2019
Page 3

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

Violation(s) Determined and Discovery Method								
*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation								
NERC Violation ID	Standard	Req.	VRF/VSL	Applicable Function(s)	Discovery Method* Date	Violation Start-End Date	Risk	Penalty Amount
	CIP-004-6	R3. Part 3.4	Medium/ Severe		CA		Minimal	\$1M
	CIP-004-6	R4. Part 4.1	Medium/ Moderate		CA		Minimal	
	CIP-005-5	R1. Part 1.3	Medium/ Severe		CA		Moderate	
	CIP-006-6	R1. Part 1.3	Medium/ Severe		CA		Minimal	
	CIP-006-3c	R1, R1.6. 1	Medium/ Severe				Minimal	
	CIP-007-3a	R2	Medium/ High		CA		Serious	
	CIP-007-3a	R3	Lower/ High		CA		Serious	
	CIP-007-6	R3	Medium/ Severe		CA		Serious	
	CIP-007-6	R4 Part 4.1	Medium/ Severe		CA		Serious	

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

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

[REDACTED]	CIP-007-3a	R5 Part 5.2, 5.3, 5.7	Lower/ High	[REDACTED]	CA [REDACTED]	[REDACTED]	Serious	
[REDACTED]	CIP-010-2	R2	Medium/ Severe	[REDACTED]	CA [REDACTED]	[REDACTED]	Minimal	\$1M
[REDACTED]	CIP-011-2	R1	Medium/ Severe	[REDACTED]	CA [REDACTED]	[REDACTED]	Moderate	
[REDACTED]	CIP-005-3a	R2, 2.1, 2.2	Medium/ Severe	[REDACTED]	CA [REDACTED]	[REDACTED]	Serious	

FACTS COMMON TO VIOLATIONS

[REDACTED]

The Entity and [REDACTED] entered into a Settlement Agreement to resolve 13 violations of the CIP Reliability

[REDACTED]

⁵ One violation in this case was open before the [REDACTED] Compliance Audit and is resolved in the instant Settlement Agreement.

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

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

The violations discussed herein were the result of an organizational weakness with respect to the processes and procedures The Entity had in place at the time of the Compliance Audit. The Entity has since addressed its weakness and established measures to prevent recurrence.

CIP-004-6 R3

██████ determined that The Entity did not properly retain required documentation of personnel risk assessments (PRA). The Entity did not have an attesting affidavit for one contractor identified in audit team's sample testing. In addition, the company did not verify the performance of attestations (P3.4) associated with PRAs performed by contractors.

The root cause of this violation was inadequate procedures. No Entity staff were actively involved in verifying the assessment criteria or results, and the completion of the PRA was only verified through a signed affidavit by the contractor conducting the assessment. Additionally, The Entity failed to implement the flawed procedure, which required The Entity to obtain and retain signed affidavits for completion of contractor PRAs.

██████ determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted its 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 that it had completed all mitigation activities. ██████ verified that The Entity had completed all mitigation activities as of October 25, 2018. Attachments 4b and 4c provide specific information on ██████ verification of The Entity's completion of the activities.

CIP-004-6 R4

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

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

██████ determined that The Entity did not have sufficient controls over the distribution of physical keys, which led to the improper provisioning of physical keys to employees without authorization.

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

██████ determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted its 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.

The Entity certified that it had completed all mitigation activities. ██████ verified that The Entity had completed all mitigation activities as of October 25, 2018. Attachments 5b and 5c provide specific information on ██████ verification of The Entity's completion of the activities.

CIP-005-5 R1

██████ determined that The Entity permitted Internet Control Message Protocol (ICMP) inbound and outbound communications through an Electronic Access Point (EAP) to its high and medium impact Bulk Electric System Cyber Systems (BCSs) without maintaining documentation supporting the reason it granted the communication access.

The root cause of this violation was insufficient procedures that lacked the granularity necessary to ensure that access rules had the need and reason clearly documented. A lack of clear guidance within the procedures allowed for multiple failures of this type, where the subject matter experts would either not address the potential access permissions on EAPs or manage the EAP configurations through their professional judgment and experience.

██████ determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted its 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.

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 that it had completed all mitigation activities. [REDACTED] verified that The Entity had completed all mitigation activities as of October 25, 2018. Attachments 6b and 6c provide specific information on [REDACTED] verification of The Entity's completion of the activities.

CIP-006-6 R1

[REDACTED] determined that The Entity did not implement two or more different physical access controls to restrict unescorted physical access into the foyer of the [REDACTED] which was classified by The Entity as a part of a Physical Security Perimeter (PSP).

The root cause for this violation was a lack of clarity in its physical security plan and inadequate procedures for how The Entity should implement access control and management, particularly in unique or complicated facilities.

[REDACTED] determined that this violation posed a minimal and not 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 its 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.

The Entity certified that it had completed all mitigation activities. [REDACTED] verified that The Entity had completed all mitigation activities as of October 25, 2018. Attachments 7b and 7c provide specific information on [REDACTED] verification of The Entity's completion of the activities.

CIP-006-3c R1

During a review of evidence provided, the [REDACTED] audit team discovered several instances where The Entity failed to record the exit time for visitors from the Physical Security Perimeter (PSP).

The root cause of this noncompliance was inadequate processes and internal controls for reviewing logs, and deficient training of escorts.

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

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

██████ determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted its 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 that it had completed all mitigation activities. ██████ verified that The Entity had completed all mitigation activities as of October 25, 2018. Attachments 8b and 8c provide specific information on ██████ verification of The Entity's completion of the activities.

CIP-007-3a R2

██████ determined that The Entity did not properly document its need to have logical network accessible ports enabled for certain of its BES Cyber Assets (BCAs). In addition, The Entity did not properly document that certain of its BCAs did not have a provision for disabling or restricting logical ports nor did it file a Technical Feasibility Exception (TFE) to document the mitigating measures for these BCAs.

The root cause for this noncompliance was inadequate processes including a lack of controls to ensure it enabled only logical network accessible ports and services deemed necessary, gathering of appropriate vendor documentation to support when they could not be technically disabled or filed in an appropriate TFE.

██████ determined that this violation posed a serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted its 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.

The Entity certified that it had completed all mitigation activities. ██████ verified that The Entity had completed all mitigation activities as of May 8, 2019. Attachments 9b and 9c provide specific information on ██████ verification of The Entity's completion of the activities.

CIP-007-3a R3

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

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

██████ determined that The Entity's documented processes of cyber security patch management for its BES Cyber Assets did not include procedures for evaluating the applicability of new security patches prior to installation that were consistent with the Standard Requirements. Specifically, The Entity's process neither appropriately assessed the applicability of new security patches for Cyber Assets nor provided for the retention of tracking records that support the performance of tests of patches.

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

██████ determined that this violation posed a serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted its 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 that it had completed all mitigation activities. ██████ verified that The Entity had completed all mitigation activities as of May 8, 2019. Attachments 10b and 10c provide specific information on ██████ verification of The Entity's completion of the activities.

CIP-007-6 R3

██████ determined that The Entity implemented a network system option through an intrusion detection and prevention system (IDPS) for the Cyber Assets that could not support Cyber Asset-based malware prevention software. In this instance, the eight (8) Cyber Assets identified by the audit team were outside of the Electronic Security Perimeter (ESP), and thus were not available for protection by the network solution The Entity had implemented.

The root cause for this violation was inadequate processes and a lack of controls around the deployment of malware prevention protections. Where The Entity did not utilize Cyber Asset-level malware prevention at the suggestion of device vendors, The Entity also did not research or utilize a BES Cyber Systems approach for malware prevention.

██████ determined that this violation posed a serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

NERC Notice of Penalty
The Entity
May 30, 2019
Page 10

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

The Entity submitted its 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 that it had completed all mitigation activities. [REDACTED] verified that The Entity had completed all mitigation activities as of May 8, 2019. Attachments 11b and 11c provide specific information on [REDACTED] verification of The Entity's completion of the activities.

CIP-007-6 R4

[REDACTED] determined that The Entity implemented a network system option through an intrusion detection and prevention system (IDPS) for the Cyber Assets that could not support Cyber Asset-based malware prevention software. In this instance, the eight (8) Cyber Assets identified by the audit team were outside of the Electronic Security Perimeter (ESP), and were not available for monitoring and event logging by the network solution The Entity had implemented.

The root cause for this violation was inadequate processes and a lack of controls around the proper identification of a Cyber Assets ability to perform event logging and generation of alerts.

[REDACTED] determined that this violation posed 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 its 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 that it had completed all mitigation activities. [REDACTED] verified that The Entity had completed all mitigation activities as of May 8, 2019. Attachments 12b and 12c provide specific information on [REDACTED] verification of The Entity's completion of the activities.

CIP-007-3a R5

[REDACTED] determined that The Entity did not properly identify individuals who had authorized access to shared accounts. In addition, The Entity did not file a TFE for its inability to support alerting for unsuccessful login attempts on a BCA, nor demonstrate its implementation of compensating and/or mitigating measures on the BCA.

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

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

The root cause for this violation was inadequate processes and a lack of controls for system access controls, including identifying and documenting shared accounts; and, limiting the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful authentication attempts.

██████ determined that this violation posed a serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted its 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 that it had completed all mitigation activities. ██████ verified that The Entity had completed all mitigation activities as of May 8, 2019. Attachments 13b and 13c provide specific information on ██████ verification of The Entity's completion of the activities.

CIP-010-2 R2

██████ determined that The Entity did not have documented processes for investigating detected unauthorized changes to baseline configurations of its BCAs, as required.

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

██████ determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted its 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 14a.

The Entity certified that it had completed all mitigation activities. ██████ verified that The Entity had completed all mitigation activities as of October 25, 2018. Attachments 14b and 14c provide specific information on ██████ verification of The Entity's completion of the activities.

CIP-011-2 R1

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

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

██████ determined that The Entity did not properly identify a storage area network Cyber Asset used to store security configurations of its BCAs as a BES Cyber System Information (BCSI) storage location.

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

██████ determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted its 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 15a.

The Entity certified that it had completed all mitigation activities. ██████ verified that The Entity had completed all mitigation activities as of May 8, 2019. Attachments 15b and 15c provide specific information on ██████ verification of The Entity's completion of the activities.

CIP-005-3a R2

██████ determined that The Entity's documentation was insufficient to demonstrate that it uses an access control model such that explicit access permissions are specified. In addition, The Entity's documentation was insufficient to demonstrate: 1) that it enabled only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter; and 2) that The Entity documented, individually or by specified grouping, the configuration of those ports and services.

The root cause for this violation was inadequate processes and a lack of controls around access control such that explicit access permissions are specified.

██████ determined that this violation posed a serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3 includes the facts regarding the violation that ██████ considered in its risk assessment.

The Entity submitted its 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 16a.

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

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

The Entity certified that it had completed all mitigation activities. [REDACTED] verified that The Entity had completed all mitigation activities as of October 26, 2016. Attachments 16b and 16c provide specific information on [REDACTED] verification of The Entity's completion of the activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, [REDACTED] has assessed a penalty of one million dollars (\$1,000,000) for the referenced violations. In reaching this determination, [REDACTED] considered the following factors:

1. [REDACTED] considered the instant violations as repeat noncompliance with the subject NERC Reliability Standards. [REDACTED] considered The Entity's compliance history with CIP-004 R4, CIP-005 R2, and CIP-007 R2, R3, R4, R5, and R6 as an aggravating factor in the penalty determination;⁶
2. The Entity had an internal compliance program at the time of the violation which [REDACTED] considered a neutral factor, as discussed in Attachment 1;
3. The Entity was cooperative throughout the compliance enforcement process;
4. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

After consideration of the above factors, [REDACTED] determined that, in this instance, the penalty amount of one million dollars (\$1,000,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction, or Enforcement Action 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

⁶ The Entity's relevant prior noncompliance with CIP-004 R4, CIP-005 R2, and CIP-007 R2, R3, R4, R5, and R6 includes: NERC Violation ID [REDACTED]

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).

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

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

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 one million dollars (\$1,000,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

- 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

⁹ 18 C.F.R. § 388.113(e)(1).

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

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

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.

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

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). 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 16

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

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.

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.

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

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

Attachments to be Included as Part of this Notice of Penalty

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

1. Settlement Agreement by and between The Region and The Entity executed April 29, 2019, included as Attachment 1;
2. [REDACTED] Final Audit Report dated June 8, 2017, included as Attachment 2
3. Details of the Violations, included as Attachment 3;
4. The Entity's Mitigation Plan designated as [REDACTED] for CIP-004-6 R3 submitted February 14, 2018, included as Attachment 4a;
5. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R3 submitted February 14, 2018, included as Attachment 4b;
6. The Region's Verification of Mitigation Plan Completion for CIP-004-6 R3 dated October 24, 2018, included as Attachment 4c.
7. The Entity's Mitigation Plan designated as [REDACTED] for CIP-004-6 R4 submitted June 19, 2018, included as Attachment 5a;
8. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R4 submitted July 20, 2018, included as Attachment 5b;
9. The Region's Verification of Mitigation Plan Completion for CIP-004-6 R4 dated October 24, 2018, included as Attachment 5c.
10. The Entity's Mitigation Plan designated as [REDACTED] for CIP-005-5 R1 submitted May 30, 2018, included as Attachment 6a;
11. The Entity's Certification of Mitigation Plan Completion for CIP-005-5 R1 submitted September 18, 2018, included as Attachment 6b;
12. The Region's Verification of Mitigation Plan Completion for CIP-005-5 R1 dated May 8, 2018, included as Attachment 6c.
13. The Entity's Mitigation Plan designated as [REDACTED] for CIP-006-6 R1 submitted February 26, 2018, included as Attachment 7a;
14. The Entity's Certification of Mitigation Plan Completion for CIP-006-6 R1 submitted May 8, 2018, included as Attachment 7b;
15. The Region's Verification of Mitigation Plan Completion for CIP-006-6 R1 dated October 28, 2018, included as Attachment 7c.

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

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

16. The Entity's Mitigation Plan designated as [REDACTED] for CIP-006-3c R1 submitted May 24, 2018, included as Attachment 8a;
17. The Entity's Certification of Mitigation Plan Completion for CIP-006-3c R1 submitted June 11, 2018, included as Attachment 8b;
18. The Region's Verification of Mitigation Plan Completion for CIP-006-3c R1 dated October 24, 2018, included as Attachment 8c.
19. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-3a R2 submitted May 24, 2018, included as Attachment 9a;
20. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R2 submitted August 17, 2018, included as Attachment 9b;
21. The Region's Verification of Mitigation Plan Completion for CIP-007-3a R2 dated May 7, 2019, included as Attachment 9c.
22. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-3a R3 submitted June 19, 2018, included as Attachment 10a;
23. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R3 submitted September 28, 2018, included as Attachment 10b;
24. The Region's Verification of Mitigation Plan Completion for CIP-007-3a R3 dated May 7, 2019, included as Attachment 10c.
25. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-6 R3 submitted May 30, 2018, included as Attachment 11a;
26. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R3 submitted August 17, 2018, included as Attachment 11b;
27. The Region's Verification of Mitigation Plan Completion for CIP-007-6 R3 dated May 8, 2019, included as Attachment 11c.
28. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-6 R4 submitted May, 30, 2018, included as Attachment 12a;
29. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R4 submitted August 17, 2018, included as Attachment 12b;
30. The Region's Verification of Mitigation Plan Completion for CIP-007-6 R4 dated May 8, 2019, included as Attachment 12c.
31. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-3a R5 submitted June 19, 2018, included as Attachment 13a;

NERC Notice of Penalty
The Entity
May 30, 2019
Page 19

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

32. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R5 submitted January 2, 2019, included as Attachment 13b;
33. The Region's Verification of Mitigation Plan Completion for CIP-007-3a R5 dated May 8, 2019, included as Attachment 13c.
34. The Entity's Mitigation Plan designated as [REDACTED] for CIP-010-2 R2 submitted May 23, 2018, included as Attachment 14a;
35. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R2 submitted May 29, 2018, included as Attachment 14b;
36. The Region's Verification of Mitigation Plan Completion for CIP-010-2 R2 dated October 24, 2018, included as Attachment 14c.
37. The Entity's Mitigation Plan designated as [REDACTED] for CIP-011-2 R1 submitted May 23, 2018, included as Attachment 15a;
38. The Entity's Certification of Mitigation Plan Completion for CIP-011-2 R1 submitted May 31, 2018, included as Attachment 15b;
39. The Region's Verification of Mitigation Plan Completion for CIP-011-2 R1 dated May 18, 2019, included as Attachment 15c.
40. The Entity's Mitigation Plan designated as [REDACTED] for CIP-005-3a R2 submitted January 26, 2015, included as Attachment 16a;
41. The Entity's Certification of Mitigation Plan Completion for CIP-005-3a R2 submitted December 17, 2015, included as Attachment 16b; and
42. The Region's Verification of Mitigation Plan Completion for CIP-005-3a R2 dated October 25, 2016, included as Attachment 16c.

NERC Notice of Penalty
The Entity
May 30, 2019
Page 20

**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:

<p>*Persons to be included on the Commission’s service list are indicated with an asterisk. NERC requests waiver of the Commission’s rules and regulations to permit the inclusion of more than two people on the service list.</p>	<p>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</p> <p>Jill Goatcher* Associate Counsel North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile jill.goatcher@nerc.net</p>
---	---

NERC Notice of Penalty
The Entity
May 30, 2019
Page 21

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

cc: The Entity



Attachments

Attachment 1

Settlement Agreement by and between The
Region and The Entity executed April 29, 2019

SETTLEMENT AGREEMENT

BETWEEN

AND

I. INTRODUCTION

1. The [REDACTED] and [REDACTED] enter into this Settlement Agreement (Agreement) to resolve all outstanding Alleged Violations by [REDACTED] of the below-referenced Reliability Standards and Requirements.¹

Reliability Standard	Requirement	[REDACTED] Tracking No.	NERC Tracking No.
CIP-005-3a	R2.	[REDACTED]	[REDACTED]
CIP-004-6	R3. Part 3.4	[REDACTED]	[REDACTED]
CIP-004-6	R4. Part 4.1	[REDACTED]	[REDACTED]
CIP-005-5	R1. Part 1.3	[REDACTED]	[REDACTED]
CIP-006-6	R1. Part 1.3	[REDACTED]	[REDACTED]
CIP-006-3c	R1.6.1	[REDACTED]	[REDACTED]
CIP-007-3a	R2.	[REDACTED]	[REDACTED]
CIP-007-3a	R3.	[REDACTED]	[REDACTED]
CIP-007-6	R3.	[REDACTED]	[REDACTED]
CIP-007-6	R4.	[REDACTED]	[REDACTED]
CIP-007-3a	R5.	[REDACTED]	[REDACTED]
CIP-010-2	R2.	[REDACTED]	[REDACTED]
CIP-011-2	R1.	[REDACTED]	[REDACTED]

2. The Parties enter into this Agreement, including Attachment A, for the sole purpose of resolving all outstanding issues related to the violations and the associated extent of conditions and Mitigation Plans. The Parties have worked extensively to determine what violations may have occurred and, more importantly, how best to ensure that progress is made to improve [REDACTED] processes for compliance. The Agreement and Attachment A have been drafted from the standpoint of the [REDACTED] review and its determinations rather than from a stipulated set of facts or joint determinations between the Parties. In the interest

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

of reaching a resolution of the matters set forth herein, the Parties enter into this Agreement on the basis that: (a) [REDACTED] make a payment in the amount referenced below in Paragraph 16 below; and (b) [REDACTED] continues to work to improve its compliance processes, taking into account the [REDACTED] determinations set forth in this Agreement and Attachment A, but without stipulation by [REDACTED] as to any facts or statements in this Agreement or Attachment A. [REDACTED] neither admits nor denies the facts or statements in this Agreement or Attachment A or that they constitute violations of the above-referenced Reliability Standard Requirements.

II. OVERVIEW OF [REDACTED]

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

III. EXECUTIVE SUMMARY

8. This Agreement resolves thirteen (13) violations² of Critical Infrastructure Protection (CIP) Reliability Standards related to [REDACTED]³ [REDACTED]
9. [REDACTED] determined that [REDACTED] was in violation CIP Reliability Standards in multiple areas of security and compliance, most seriously in systems security management (CIP-007), including physical and electronic security. [REDACTED] also found [REDACTED] had issues with personnel and training, configuration change management and vulnerability assessments, and information protection. [REDACTED] determined that five (5) posed a minimal risk the bulk power system (BPS), two (2) posed a moderate risk to the BPS, and five (5) posed a serious and substantial risk to the BPS. [REDACTED] posed a serious and substantial risk to the BPS. The details of the 13 violations are provided in Attachment A to this agreement.
10. [REDACTED] drafted Mitigation Plans that address each violation and prevent recurrence. Overall, [REDACTED] submitted 13 Mitigation Plans that collectively include over 150 milestones. For each violation, [REDACTED] conducted an extent of condition review to determine the scope, root causes, and contributing causes. Inadequate processes and procedures were the root cause for all of the violations [REDACTED]. The root cause for the preexisting violation was an inadequate installation/design configuration of the firewalls.
11. Based on the mix of serious, moderate, and minimal risk posed by the violations and the repeat nature of some of the violations, [REDACTED] determined a monetary penalty of \$1,000,000.00 to be applicable to [REDACTED]

IV. ADJUSTMENT FACTORS

12. In addition to the facts and circumstances stated above, the following factors were considered by the [REDACTED] in the penalty determination:

² Each Violation is described as a violation, regardless of its procedural posture and whether it is a possible, alleged, or confirmed violation.

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

Internal Compliance Program

13. [REDACTED] internal compliance program (ICP) was reviewed and considered to be a neutral factor in the penalty determination. [REDACTED] has a documented ICP, the most recent revision is [REDACTED], which includes components, processes, responsibilities, and training needed to ensure [REDACTED] maintains compliance. However, in this case it did not effectively enable [REDACTED] to prevent and detect the violations.

Cooperation

14. [REDACTED] cooperation during the audit and Agreement process was considered and determined to be a neutral factor. [REDACTED] 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, whether the facts of these violations constitute repetitive infractions was considered. [REDACTED] has prior violations of CIP-004 R4, CIP-005 R2, and CIP-007 R2, R3, R4, R5, and R6 that are similar to the current violations and were considered aggravating factors in determining the penalty.

V. PENALTY

16. Based upon the foregoing, [REDACTED] agreed to pay a monetary penalty of \$1,000,000.00 in total to [REDACTED]
17. [REDACTED] shall remit the penalty payment to [REDACTED] via check 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.
18. If [REDACTED] 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

19. 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.
20. [REDACTED] shall report the terms of all settlements of compliance matters to NERC. NERC will review the Agreement for the purpose of evaluating its consistency with other settlements entered into for similar violations or under similar circumstances. Based on this review, NERC will either approve or reject this Agreement. If NERC rejects the Agreement, NERC will provide specific written

reasons for such rejection and [REDACTED] will attempt to negotiate with [REDACTED] a revised settlement agreement that addresses NERC's concerns. If a settlement cannot be reached, the enforcement process will continue to conclusion. If NERC approves the Agreement, NERC will (a) report the approved settlement to the Commission for review and approval by order or operation of law and (b) publicly post the violations and the terms provided for in this Agreement in accordance with applicable FERC regulations and the NERC Rules of Procedure.

21. This Agreement binds the Parties upon execution and may only be altered or amended by written agreement executed by the Parties. [REDACTED] expressly waives its right to any hearing or appeal concerning any matter set forth herein, unless and only to the extent that [REDACTED] contends that any NERC or Commission action constitutes a material modification to this Agreement.
22. [REDACTED] reserves all rights to initiate enforcement action against [REDACTED] in accordance with the NERC Rules of Procedure in the event that [REDACTED] fails to comply with any of the terms or conditions of this Agreement. [REDACTED] retains all rights to defend against such action in accordance with the NERC Rules of Procedure.
23. [REDACTED] consents to [REDACTED] future use of this Agreement for the purpose of assessing the factors within the NERC Sanction Guidelines and applicable Commission orders and policy statements, including, but not limited to, the factor evaluating [REDACTED] compliance history. Such use may be in any enforcement action or compliance proceeding undertaken by NERC or any Regional Entity or both, provided however that [REDACTED] does not consent to the use of the conclusions, determinations, and findings set forth in this Agreement as the sole basis for any other action or proceeding brought by NERC or any Regional Entity or both, nor does [REDACTED] consent to the use of this Agreement by any other party in any other action or proceeding.
24. [REDACTED] affirms that the information provided during the audit, and ultimately leading to this Agreement, is 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 [REDACTED] to [REDACTED] during any [REDACTED] interaction with [REDACTED] relating to the subject matter of this Agreement.
25. Upon execution of this Agreement, the Parties stipulate that any requirements stated in Section 5.3 of the Compliance Monitoring and Enforcement Program ("CMEP") will be deemed to have been satisfied or waived by this Agreement.
26. 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.
27. 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.

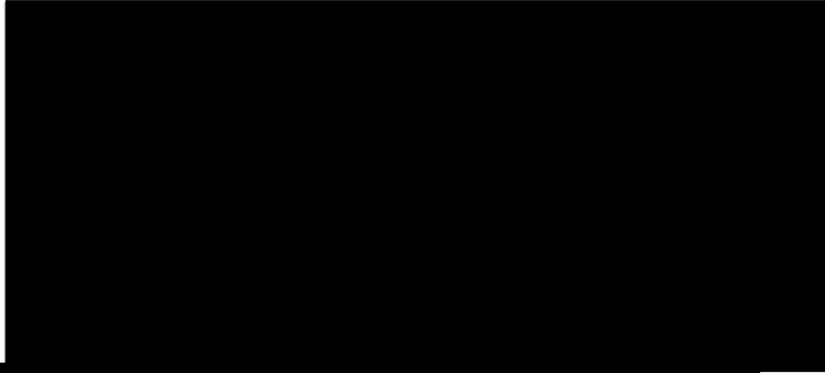
28. The Agreement may be signed in counterparts.
29. This Agreement is executed in duplicate, each of which so executed shall be deemed to be an original.

[SIGNATURE PAGE TO FOLLOW]⁴

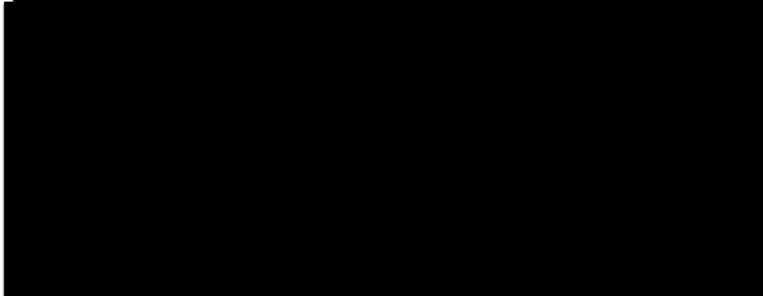
[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

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

Agreed to and accepted by:



4/29/19



4/26/19
Date

Attachment 2

Final Audit Report dated

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]

[REDACTED]

[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.

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.

█████ acknowledged the issues and consented that it did not have an attesting affidavit for one contractor identified in audit staff's sample testing.¹¹ Because the audit staff's review involved a sample of PRA records out of a larger population, the audit team believes that review of a larger number of records may have revealed additional retention and verification errors.

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. ██████

Pertinent Guidance

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

Background

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 it [REDACTED]

¹¹ See evidence artifact: CIP-004-R3-L11-06 Evidence-CEII.pdf at 1 – 3.

¹² CIP-004-6 at 15-19.

¹³ See the Administrator Properties screen on page 9, Index 5 of CIP-004-R4-L2-04 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.

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

Additionally, the audit team discovered that [REDACTED] key administrator 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

[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.

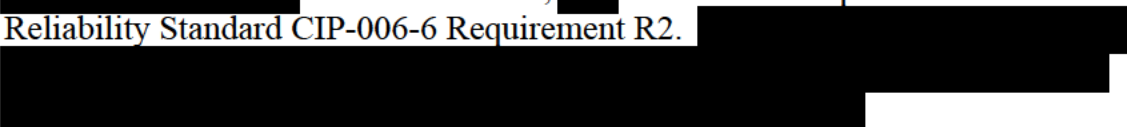
Background

[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.

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

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.

█████ maintained visitor access logs that documented access into its PSPs. The audit team reviewed the access logs at █████ █████ PSP and found that on several occasions visitors signed into the PSP, entering data for the time-in field, but the time-out fields for these visitors were not populated in the logs.²⁰ CIP-006-6 R2.2 requires that █████ log visitors' entries into and exits out of the PSP. Moreover, the log must be populated with the date and time of the initial entry and last exit. █████ visitor access logs were deficient and not consistent with this Reliability Standard requirement.

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

██████ did not properly document its need to have logical network accessible ports enabled for certain of its BES Cyber Assets. In addition, ██████ did not properly document that certain of its BES Cyber Assets did not have a provision for disabling or restricting logical ports. As a result, ██████ was not in compliance with the CIP Reliability Standard CIP-007-6 Requirement R1. ██████

Pertinent Guidance

CIP-007-6 R1.1 requires Responsible Entities to implement one or more documented process(es) that, 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.

CIP-007-6 R1.1 requires the “use of compensating measures 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, or part thereof,” when Strict Compliance is not technically feasible.²¹ Furthermore, the entity is required to file a TFE with their Regional Entity or NERC that describes the covered asset and the mitigating measures.²²

²⁰ See evidence artifact: CIP-006-R2-L2-02 Evidence-CEII.pdf at 22.

²¹ 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).

²² *Id.* at 6 (Apr. 1, 2016) and at 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.

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]

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.*

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.

feasible, either: (1) Limit the number of unsuccessful authentication attempts; or (2) Generate alerts after a threshold of unsuccessful authentication attempts.

Background

█████ implementation of Interactive Remote Access (IRA) relies heavily upon Active Directory (AD).³² Audit staff analyzed a list of █████ AD groups that received remote access to █████ Cyber Systems and Assets. For each group, █████ stated whether members of the group had corresponding equivalent access approval roles in its █████ and █████ provided the name of the role.³³ █████ admitted that no █████ access role existed for the AD group listed as “Domain Admin” in the █████ Domain.³⁴ Specifically, an █████ role for the shared account “█████” was not created as part of █████ transition to CIP version 5. However, in accordance with the standard, individuals in █████ Domain Admin group should have been given access roles in the █████ with established authorized access limitations. █████ addressed this issue in █████ and submitted an updated spreadsheet to audit staff showing user access information for the shared account “█████”³⁵

In addition, [REDACTED] acknowledged that members in its AD group listed as “Transmission” in the AD Domain column may not be accurately identified. [REDACTED] explained that it would implement procedures to correct this deficiency. [REDACTED]

³² Active Directory is a directory service that Microsoft developed for Windows domain networks. A directory service provides information on what functions or resources a user has on a communication network.

33

³⁴ See evidence artifact: CIP-004-R4-L13-05 Evidence-CEII.pdf at 2.

³⁵ See evidence artifact: IM-CIP-004-EVD-CIP-004-R4-L13-05-Domain Admin-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.

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.

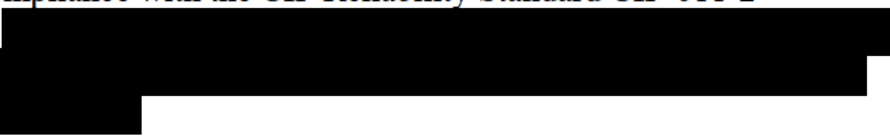
Document must be treated as CEII until the CEII Coordinator removes the designation.

[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 power delivery 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_PD-CIP-002-INS-BCS_Categorization-CEII.pdf and (2) CIP-002-R1-L1-03_PD-CIP-002-EVD-BCS_List [REDACTED]-CEII.xlsm.

⁴² See evidence artifact: CIP-002-R1-L1-03_PD-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. For example, the Production Lead Office and Restroom off the Control Room at [REDACTED] is not considered to be part of the PSP in the drawings, but should have been marked as such.⁴⁵ In addition, the general office [REDACTED] cabinets are not shown in sufficient detail in that drawing.⁴⁶ [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.LCD.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 PWC, three as [REDACTED], and one as [REDACTED]
[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

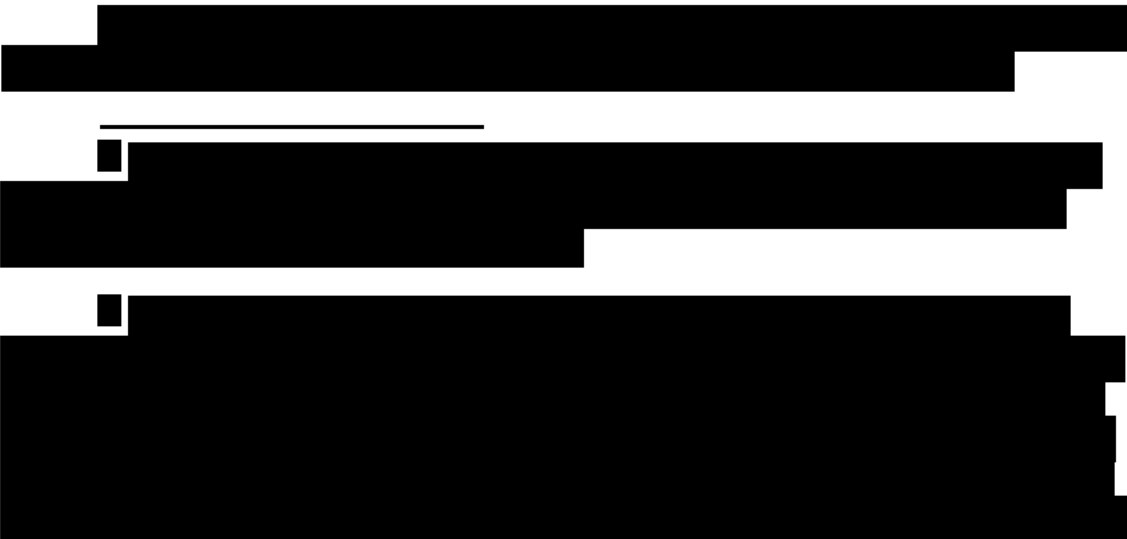
[CEII]



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 [REDACTED] 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.

Attachment 3

Details of the Violations

CONFIDENTIAL
NOC-2623

\$1,000,000

██████████ "the Entity") – ██████████

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
██████████	CIP-004-6	R3. Part 3.4	Medium	Severe	07/01/2016 (enforceable date of Standard when the Entity did not properly retain required documentation of personnel risk assessments (PRA) that were performed)	2/28/2018 (when the Entity completed the mitigation plan)	Audit	02/28/2018	10/25/2018
Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.			<p>██████████ was in violation of CIP-004-6 R3. The Region later determined the Entity was specifically in violation of CIP-004-6 R3, Part P3.4.</p> <p>The Entity did not properly retain required documentation of personnel risk assessments (PRA). The Entity did not have an attesting affidavit for one contractor identified ██████████. In addition, the company did not verify the performance of attestations (P3.4) associated with PRAs performed by contractors.</p> <p>During a review of evidence provided, the ██████████ discovered instances where the Entity failed to follow its required documented procedure to acquire and retain documentation supporting the performance of PRAs conducted by its contractors. The documented program required the Entity 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.</p> <p>As of August 19, 2016, the Entity had ██████████ with access to protected Cyber Assets. Since no contractor processes for conducting PRAs were verified, this would conclude that just over 11% of those with Cyber Asset access had not been properly vetted as required.</p> <p>Post audit, the Entity conducted an extent of condition assessment to determine the scope of this violation. The Entity did not discover any additional instances of noncompliance where it did not retain proper PRA documentation.</p> <p>The root cause of this violation was inadequate procedures. No Entity staff were actively involved in verifying the assessment criteria or results, and the completion of the PRA was only verified through a signed affidavit by the contractor conducting the assessment. Additionally, the Entity failed to implement the flawed procedure, which required the Entity to obtain and retain signed affidavits for completion of contractor PRAs.</p>						
Risk Assessment			<p>This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>Specifically, the Entity's failure to verify the performance of attestations associated with PRAs performed by contractors and retain appropriate documentation could lead to inappropriate access by unqualified individuals with malicious intent being granted to High Impact BES Cyber Systems and potentially miss refreshes of PRAs on required dates. This inappropriate access could have allowed malicious actions to occur causing damage resulting in possible disruptions or load losses to occur potentially degrading the BPS and create a condition where a broad and cascading outage could occur.</p> <p>This risk was reduced because the Entity's contract companies were performing PRAs using a set of criteria specified in the supplemental terms and conditions for each agency to conform with the requirements of the Standard.</p> <p>No events or adverse consequences occurred and thus no actual harm is known to have occurred.</p>						
Mitigation			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none">1) 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;2) developed and documented controls to ensure contractor and service vendor PRA process was implemented and documented;3) developed a training program for contractor and services PRAs;4) implemented updated PRA procedure;5) performed an extent of condition assessment; and6) added "training" section to the PRA procedure that defined who would be required to take training on the PRA process.						

██████████ "the Region")

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-004-6	R3. Part 3.4	Medium	Severe	07/01/2016 (enforceable date of Standard when the Entity did not properly retain required documentation of personnel risk assessments (PRA) that were performed)	2/28/2018 (when the Entity completed the mitigation plan)	Audit	02/28/2018	10/25/2018
Other Factors			The Region considered the Entity’s CIP-004-6 (R3) compliance history in determining the penalty. The Region determined that the Entity's compliance history should not serve as a basis for aggravating the penalty because the facts and circumstances are different.						

CONFIDENTIAL
NOC-2623

\$1,000,000

“the Entity”) –

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-004-6	R4. Part 4.1	Medium	Moderate	07/01/2016 (enforceable date of Standard when the Entity did not have sufficient controls over the distribution of physical keys, which led to the improper provisioning of physical keys to employees without authorization)	03/05/2018 (when the Entity corrected the access and tracking issues, updated the procedures to prevent reoccurrence, and trained appropriate personnel)	Audit	03/05/2018	10/25/2018
Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.			<p>was in violation of CIP-004-6 R4. The Region later determined that the Entity was in violation of CIP-004-6 R4 Part 4.1.</p> <p>The Entity did not have sufficient controls over the distribution of physical keys, which led to the improper provisioning of physical keys to employees without authorization.</p> <p>During the audit, the audit team found the Entity key administrator (the individual responsible for distribution of physical access keys to individuals with authorized unescorted physical access), was not authorized for access to the PSPs that the physical access keys controlled. The Entity later informed the Region that the key administrator did have authorized unescorted access permissions.</p> <p>Additionally, during observations of work practices after analyzing the Entity’s access management policies and procedures, the audit team found that the Entity did not track access or review access for the domain administrator accounts to Bulk Electric System Cyber System Information (BCSI). The Region determined the Entity’s failure to track or review access to the domain accounts of this violation was best suited to be addressed under (CIP-007-3a R5).</p> <p>The Entity completed an extent of condition with the following results:</p> <ol style="list-style-type: none">1) For substations, the Entity had . The Entity reported that the key assessment inventory portion of the extent of condition efforts found all personnel assigned a key had a key, but some keys were noted as not being in circulation and being in inventory but could not be located.2) In power plants , and the Entity noted no anomalies during the assessment.3) In control center and data center environments, , and the Entity noted no anomalies during the assessment.4) The Entity identified one (1) instance where the key administrator assigned a physical access key for facilities containing High Impact BCSs to an individual who was authorized for unescorted physical access; however, this key was provided to an unauthorized project manager employee to hand-deliver to the authorized individual at the back-up control center. Approximately five hours later, on the same day, the project manager delivered the key to the authorized individual. <p>The root cause for this violation was identified as insufficient procedures that lacked specific details on how to manage physical access keys.</p>						
Risk Assessment			<p>This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>The failure to properly assign and track physical 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.</p> <p>The unauthorized project manager employee was an employee in good standing, with a valid PRA, who had been with the Entity for over eleven years.</p> <p>This risk was reduced, however, as any access made using a physical access override key at any sites containing medium or high BCSs would result in a forced entry alarm to corporate security for immediate assessment. Further, full time, armed security staff secure the facilities containing High Impact BCSs.</p> <p>No events or adverse consequences occurred and thus no actual harm is known to have occurred.</p>						
Mitigation			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none">1) created a new role in the for an ‘the Admin ID’ within the the Entity’s domain;						

“the Region”)

CONFIDENTIAL
NOC-2623

\$1,000,000

“the Entity”) –

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-004-6	R4. Part 4.1	Medium	Moderate	07/01/2016 (enforceable date of Standard when the Entity did not have sufficient controls over the distribution of physical keys, which led to the improper provisioning of physical keys to employees without authorization)	03/05/2018 (when the Entity corrected the access and tracking issues, updated the procedures to prevent reoccurrence, and trained appropriate personnel)		03/05/2018	10/25/2018
			<p>2) removed “physical” keys from the [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 (AAMs) in the area “physical” key control log. Compared Area Access Managers (AAMs) “physical” key control logs to [REDACTED] custodian “physical” key control log to ensure all “physical” keys are logged.</p> <p>3) validated Information Technology (IT) “physical” key custodians, their “physical” key custodian roles, and the “physical” key distribution process. Ensured roles were 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.</p> <p>4) created separate roles in [REDACTED]. Verified that no CIP access role in [REDACTED] provides both physical and Cyber Asset access.</p> <p>5) updated the “physical” key distribution procedure for [REDACTED];</p> <p>6) performed an extent of condition assessment;</p> <p>7) 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] roles;</p> <p>8) verified that [REDACTED] roles exist for [REDACTED] for those responsible for managing “physical” keys. Create [REDACTED] roles for “physical” keys in [REDACTED]</p> <p>9) trained “physical” key custodians on the responsibilities associated with [REDACTED] CIP access verification process for controlling “physical” keys;</p> <p>10) revised and implemented the IT “physical” key control procedure. Documented the approved “physical” key custodians. Revised the IT “physical” key distribution process to confirm that it includes a statement that “physical” keys are only provided to individuals with authorized unescorted physical access to PSPs and are assigned the “physical” key custodian role in EAMS. Revised documentation for “physical” key authorizations and distribution to include control processes.</p> <p>11) remediated any discrepancies found in the Extent of Condition performed in milestone 6;</p> <p>12) reviewed initial root causes identified during the development of Mitigation Plan, and verify that corrective measures have been implemented for root causes and contributing factors. Document if additional root causes or contributing factors were found through implementation of corrective measures; and, document any additional preventive or detective controls identified that need to be implemented.</p> <p>13) created an enterprise-wide “physical” key management process for Medium and High Impact PSPs; and</p> <p>14) 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 enterprise-wide “physical” key distribution process and retire the individual Business Unit’s processes.</p>						
Other Factors			The Region considered the Entity’s CIP-004-6 (R4) compliance history an aggravating factor in determining the penalty.						

“the Region”)

Confidential Settlement Agreement

CIP

CONFIDENTIAL
NOC-2623

\$1,000,000

“the Entity”) –

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-005-5	R1. Part 1.3	Medium	Severe	07/01/2016 (enforceable date of Standard when the Entity permitted unnecessary inbound and outbound communication through an Electronic Access Point (EAP) to its high and medium impact BCSs without maintaining documentation supporting the reason it granted the communication access)	9/18/2018 (when the Entity completed the mitigation plan)	Audit	9/18/2018	5/8/2019
Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.			<p>was in violation of CIP-005-5 R1. The Region later determined the Entity was specifically in violation of CIP-005-5 R1, Part 1.3.</p> <p>The Entity permitted Internet Control Message Protocol (ICMP) inbound and outbound communications through an Electronic Access Point (EAP) to its high and medium impact Bulk Electric System Cyber Systems (BCSs) without maintaining documentation supporting the reason it granted the communication access.</p> <p>The Audit team observed the Entity subject matter experts use ICMP to communicate from within the Electronic Security Perimeter (ESP) to multiple external servers. The Entity could not provide the Audit team documentation supporting or documenting the need for having such inbound and access permission enabled.</p> <p>The Entity conducted an extent of condition assessment to establish scope of this violation for the specific ICMP aspect. Out of high and medium impact EAPs in service, the Entity identified two (2) high impact and seven (7) medium impact EAPs as needing the ICMP rule disabled. For those other EAPs where ICMP was determined to be necessary, the Entity documented justification for the inbound and outbound access permissions.</p> <p>The root cause of this violation was insufficient procedures that lacked the granularity necessary to ensure that access rules had the need and reason clearly documented. A lack of clear guidance within the procedures allowed for multiple failures of this type, where the subject matter experts would either not address the potential access permissions on EAPs or manage the EAP configurations through their professional judgment and experience.</p>						
Risk Assessment			<p>This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>Specifically, the Entity’s failure to document the business need for allowing ICMP access both inbound and outbound could have allowed unknown personnel the ability to determine the existence of hosts within the protection of the ESP. Such information could allow an intruder to make use of such information in a Cyber attack and could increase the number of attack vectors to BCSs within the Entity's networks (i.e., ESP).</p> <p>The risk was reduced because the Entity secured the BCSs within an established ESP and PSP, both with real-time monitoring and alerting.</p> <p>No events or adverse consequences occurred and thus no actual harm is known to have occurred.</p>						
Mitigation			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none">1) performed an extent of condition to mitigate ICMP non-compliance deficiencies identified in the audit report for Medium Impact BCS EAPs;2) performed an extent of condition to mitigate ICMP non-compliance deficiencies identified in the audit report for High Impact BCS EAPs;3) updated the current EAP rule guidelines for Medium and High Impact BCSs;4) performed an extent of condition to develop a complete inventory list of existing documentation. The inventory of documentation will include policies, procedures, work instructions, drawings, implementation evidence templates, and business justification for BCS EAP rules;5) performed an extent of condition of all the High Impact BCS EAPs, which will include those used in the performance of the to identify “high risk”, per the guidelines developed in milestone 3, and classified each into categories;6) performed an extent of condition to identify and document all inbound and outbound access permissions and denials and the associated business justification for all High and Medium Impact EAPs;7) performed an extent of condition to determine whether all High and Medium Impact BCAs, (and their associated Protected Cyber Assets (PCAs)), reside within an ESP, and all external connectivity is through an EAP that is identified on an ESP diagram;						

“the Entity”) –

CONFIDENTIAL
NOC-2623

\$1,000,000

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-005-5	R1. Part 1.3	Medium	Severe	07/01/2016 (enforceable date of Standard when the Entity permitted unnecessary inbound and outbound communication through an Electronic Access Point (EAP) to its high and medium impact BCSs without maintaining documentation supporting the reason it granted the communication access)	9/18/2018 (when the Entity completed the mitigation plan)	Audit	9/18/2018	5/8/2019
			8) worked with the inventory report from the extent of condition in Milestone 4, IT determined how the evidence should be structured, and how the implementation evidence template will be a repeatable, sustainable process; 9) used the inventory list from the extent of condition in Milestone 6, and the guidance documentation and template(s) created in Milestone 8, to determine which firewall rules and business justifications, (inclusive of those related to temporary rules), meet the requirements listed within the guidance document. 10) used the identified BCS EAP inventory list for all High and Medium Impact BCS at Control Centers, perform an extent of condition to verify that there is at least one method of detecting malicious communication for all inbound and outbound communications; 11) performed a Root Cause Analysis; 12) created comprehensive enterprise-wide Policies, Procedures and Work Instructions for current and new ESPs and/or devices; 13) developed training for new and updated documentation and implementation evidence templates, and provide training to Personnel; 14) communicated to all SMEs and users, information about the new or updated policies, procedures and work instructions; and 15) corrected any deficiency found in previous milestones.						
Other Factors			The Entity’s CIP-005-5 (R1) compliance history was not an aggravating factor in determining the penalty.						

CONFIDENTIAL
NOC-2623

\$1,000,000

“the Entity”) –

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-006-6	R1. Part 1.3	Medium	Severe	07/01/2016 (enforceable date of Standard when the Entity did not implement two or more different physical access controls to allow unescorted physical access into the foyer of the LBCC Physical Security Perimeter (PSP) as required by the Standard)	10/10/2017 (when the Entity completed the mitigation plan)	Audit	10/10/2017	10/25/2018
Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.			<p>was in violation of CIP-006-6 R1. The Region later determined the Entity was specifically in violation of CIP-006-6 R1. Part 1.3.</p> <p>The Entity did not implement two or more different physical access controls to restrict unescorted physical access into the foyer of the which was classified by the Entity as a part of a Physical Security Perimeter (PSP).</p> <p>During site visits conducted during the audit, audit team observed an emergency exit door permitted access into the when an emergency ‘request-to-access’ button on the exterior of the PSP door was pressed. The Entity modified the designated PSP by removing the door from the PSP description because the door at issue only provided access to the atrium area.</p> <p>After the audit concluded, using its CIP-002 BCS list, the Entity conducted an extent of condition assessment to establish the scope of this violation. The Entity’s corporate security staff conducted a physical walk down of all PSPs to compare the actual design noted in the physical security plan to the ‘as built’. Specifically, for each PSP access point, the Entity looked for any design where someone could access a PSP through the activation of an emergency exit method from outside of the PSP egress door. The Entity did not find any additional instances.</p> <p>The root cause for this violation was a lack of clarity in its physical security plan and inadequate procedures for how the Entity should implement access control and management, particularly in unique or complicated facilities.</p>						
Risk Assessment			<p>This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>The Entity’s 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 and impact local operations or affect operations of the BPS.</p> <p>The risk was reduced, however, because the door at issue had a loud audible siren, which would sound when the request-to-exit button was activated. Additionally, the foyer, which was a part of a PSP identified by the Entity, contained no BCSs or BCAs, and was an area that although identified as a part of the PSP, should have been removed from the diagram. Other PSP doors leading from the foyer into the backup Control Center and computer room were secured with two factor access controls. This ensured access to access BCSs or BCAs were protected at all times. The effort to remediate this issue was to re-draw the boundaries eliminating the foyer from the PSP.</p> <p>No events or adverse consequences occurred and thus no actual harm is known to have occurred.</p>						
Mitigation			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none">1) updated the PSP at the site to remove the foyer area. The Responsible Entity’s Business Unit (BU) will remove the foyer door programming from the Physical Access Control System (PACS). Following this change, the Security Operations Center will no longer monitor the foyer as a PSP;2) revised/updated the PSP drawing for the to properly illustrate the foyer area and its authentication controls;3) reviewed each High Impact PSP design by conducting a walkdown to ensure no entry by key core, push button, etc., into the PSP from an egress only door;4) corrected any egress only doors that allow entry into a High Impact PSP found during walkdown in Milestone 3;5) reviewed Enterprise-wide Physical Security Plan to determine whether design expectations related to egress only doors are described within the Physical Security Plan;6) conducted training on the design expectations for egress only doors;7) revised Procedure to include instructions that physical security drawings should be reviewed as part of a walkdown, discussed with the BU any changes or modifications that may have been made prior to the walkdown, and documented exceptions identified during the walkdown; and8) trained on the updated Procedure.						
Other Factors			<p>The Entity’s CIP-006-6 (R1) compliance history was not an aggravating factor in determining the penalty.</p>						

“the Region”)

Confidential Settlement Agreement

CIP

CONFIDENTIAL
NOC-2623

\$1,000,000

██████████ “the Entity”) – ██████████

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
██████████	CIP-006-3c	R1., R1.6.1	Medium	Severe	03/01/2015 (when the Entity did not properly maintain complete visitor access control logs for a Physical Security Perimeter. Entries missing were related to missing exit times, lack of properly identifying am/pm on entered time, and missing signatures from either the escort or visitor)	12/15/2017 (when the Entity completed the mitigation plan)	Audit	01/01/2018	10/25/2018
Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.			██████████ was in violation of CIP-006-3c R1.6.1. During a review of evidence provided, the ██████████ discovered several instances where the Entity failed to record the exit time for visitors from the Physical Security Perimeter (PSP). After the audit concluded the Entity conducted 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. The Entity assessed ██████ pages of monthly and found ██████ instances where the individual log entries were incomplete and in violation across the CIP enterprise. Most of the failures involved not capturing the a.m. or p.m. or documenting the exit time of the visitor. The root cause of this noncompliance was inadequate processes and internal controls for reviewing logs, and deficient training of escorts.						
Risk Assessment			This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The Entity’s failure to properly maintain visitor logs for access and egress from the PSP could lead to an unattended visitor remaining within a PSP and 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. No events or adverse consequences occurred and thus no actual harm is known to have occurred.						
Mitigation			To mitigate this violation, the Entity: 1) evaluated the process for reviewing visitor access logs and identified enhancements that needed to be incorporated, including creating new controls and strengthening existing controls; 2) reviewed the process for signing visitors in and out of PSPs. Reviewed the process that is utilized by those who have authorized unescorted physical access; and, identified enhancements that needed to be incorporated including creating new controls and strengthening existing controls; 3) performed an extent of condition analysis by reviewing visitor log entries to all PSPs; 4) modified visitor log process for signing visitors in-and-out of PSPs, and incorporated enhancements identified in Milestones 1 and 2 into the modified process; 5) reviewed the PSP visitor logs and identified all instances where the escort can correct deficient log entries missing required data, and close out the missing log entries; and 6) administered training with the employees and independent contractors who are responsible for monitoring, managing and reviewing visitor logs according to the revised processes.						
Other Factors			The Entity’s CIP-006-6 (R2) compliance history was not an aggravating factor in determining the penalty.						

CONFIDENTIAL
NOC-2623

\$1,000,000

“the Entity”) –

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-007-3a	R2.	Medium	High	12/19/2013 (when the Entity did not properly document its need to have logical network accessible ports enabled for certain of its BES Cyber Assets (BCAs))	8/17/2018 (when the Entity completed the mitigation plan)	Audit	8/17/2018	5/8/2019
Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.			<p>was in violation of CIP-007-6 R1. The Region later determined that the violation extended back to CIP-007-3a R2.</p> <p>The Entity did not properly document its need to have logical network accessible ports enabled for certain of its BES Cyber Assets (BCAs). In addition, the Entity did not properly document that certain of its BCAs did not have a provision for disabling or restricting logical ports nor did it file a Technical Feasibility Exception (TFE) to document the mitigating measures for these BCAs.</p> <p>The Entity, across its entire CIP enterprise, had . After the extent of condition assessment concluded, the Entity identified: two open ports and services on the GPS clock Cyber Asset without justification having the potential to impact .</p> <p>The root cause for this noncompliance was inadequate processes including a lack of controls to ensure it enabled only logical network accessible ports and services deemed necessary, gathering of appropriate vendor documentation to support when they could not be technically disabled or filed in an appropriate TFE.</p>						
Risk Assessment			<p>This violation posed a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>Specifically, the Entity’s 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. Additionally, failure to document when unnecessary port and services could not be disabled nor file an appropriate TFE leaves those open ports and services open without providing appropriate mitigation and creates an opportunity for unneeded and potentially vulnerable ports and services to be available for exploit by an individual with malicious intent. Both could impact BCS and the operation of the BES.</p> <p>The risk was reduced because all BCSs were protected in Electronic Security Perimeters and the Entity needed all the ports and services involved but failed to document justification.</p> <p>No events or adverse consequences occurred and thus no actual harm is known to have occurred.</p>						
Mitigation			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none"> 1) created an inventory list of policies, standards, procedures, and work instruction documentation for ports and services currently in effect; 2) developed an inventory list of all existing ports and services implementation evidence templates not previously identified in milestone 1; 3) determined the sustainability of existing ports and services implementation evidence templates in the inventory list created in milestone 2; 4) evaluated the inventory list created in milestone 1 of effective policies, standards, procedures, and work instruction documentation for ports and services; 5) performed an extent of condition of all enabled ports and services are documented for all applicable devices; 6) performed an extent of condition analysis to identify possible Root Cause(s) using the inventory of documentation and devices that were identified during execution of Milestones 1, 2, and 5. Possible Root Cause(s) will be identified. 7) performed a Root Cause Analysis to determine Root Cause(s) and contributing factor(s); 8) developed a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the Root Cause Analysis in milestone 7; 9) developed enterprise-wide documentation for ports and services; 10) determined Roles and Responsibilities. Identified ownership of devices by BU to ensure coverage for all ports and services; 11) reviewed the results of Milestone 10 and The CIP Senior Manager and BU Directors will agree to the designated BU ownership of devices, and their obligation to maintain processes, evidence and training for ports and services; 12) developed controls for ports and services documentation so that they are repeatable and sustainable. Controls for creating and maintaining all ports and service documentation, and implementation evidence templates, will be included in the Roles and Responsibilities’ agreements developed in Milestone 11; 13) developed implementation evidence templates for ports and services. The BUs created enterprise-wide implementation evidence templates for capturing evidence for ports and services; 						

“the Region”)

Confidential Settlement Agreement

CIP

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-007-3a	R2.	Medium	High	12/19/2013 (when the Entity did not properly document its need to have logical network accessible ports enabled for certain of its BES Cyber Assets (BCAs))	8/17/2018 (when the Entity completed the mitigation plan)	Audit	8/17/2018	5/8/2019
			14) developed training program for new and updated ports and services documentation and implementation evidence templates; 15) performed training. The BUs 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 16) implemented countermeasures, updated documentation, templates, and controls.						
Other Factors			The Entity’s CIP-007-6 (R1) compliance history was an aggravating factor in determining the penalty.						

CONFIDENTIAL
NOC-2623

\$1,000,000

“the Entity”) –

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-007-3a	R3.	Lower	High	12/19/2013 (when the Entity’s 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)	9/28/2018 (when the Entity completed the mitigation plan)	Audit	9/28/2018	5/8/2019
<p>Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.</p> <p>was in violation of CIP-007-6 R2. The Region later determined that the violation extended back to CIP-007-3a R3.</p> <p>The Entity’s 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, the Entity’s process neither appropriately assessed the applicability of new security patches for Cyber Assets nor provided for the retention of tracking records that support the performance of tests of patches.</p> <p>The Entity confirmed that it had completed an extent of condition assessment and identified additional instances where the Entity failed to identify patching sources and failed to assess security patches. The Entity 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 a patch was deployed without proper testing either within an identified test environment or within sample devices in a similar production environment.</p> <p>The Entity, across its entire CIP enterprise, had . After the extent of condition assessment concluded, the Entity identified unique devices that had at least one CIP-007-3a, R3 issue: devices that had one or more application patch source was not identified; devices that had a missed patch assessment issue; devices that had a patch not installed within the 35-day timeframe; and devices that did not have a patch mitigation plan as required.</p> <p>The root cause of this noncompliance is a lack of adequate processes and controls around the evaluation of security patches.</p>									
Risk Assessment			<p>This violation posed a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>Specifically, failure to identify, assess and test security patches could have allowed malicious individuals to exploit known vulnerabilities for an extended period. Furthermore, this presents a significant risk to its BCSs of being compromised via the unmitigated system vulnerabilities, thereby placing the reliability of the BPS at risk.</p> <p>The risk was reduced because all BCSs were protected within an Electronic Security Perimeter.</p> <p>No events or adverse consequences occurred and thus no actual harm is known to have occurred.</p>						
Mitigation			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none"> 1) created an inventory list of policies, standards, procedures, and work instruction documentation for security patch management currently in effect; 2) developed an inventory list of all existing security patch management implementation evidence templates not previously identified in milestone 1; 3) determined the sustainability of existing security patch management implementation evidence templates in the inventory list created in milestone 2. Decided how evidence should be structured, and how the security patch management implementation evidence templates could be used to create enterprise-wide security patch management evidence templates that are repeatable and sustainable; 4) evaluated the inventory list created in milestone 1 of effective policies, standards, procedures, and work instruction documentation for security patch management to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable; 5) performed an extent of condition where the BUs identified if there was documentation for the hardware and/or software patching requirements which involve monitoring of vendors for possible patches. 6) performed an extent of condition analysis to identify possible Root Cause(s) using the inventory of documentation and devices that were identified during execution of Milestones 1, 2, and 5; 7) performed a Root Cause Analysis to determine Root Cause(s) and contributing factor(s); 8) developed a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the Root Cause Analysis; 						

“the Region”)

Confidential Settlement Agreement

CIP

CONFIDENTIAL
NOC-2623

\$1,000,000

“the Entity”) –

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-007-3a	R3.	Lower	High	12/19/2013 (when the Entity’s 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)	9/28/2018 (when the Entity completed the mitigation plan)	Audit	9/28/2018	5/8/2019
			9) determined Roles and Responsibilities to identify and document ownership of devices; 10) reviewed the results of Milestone 5 and The CIP Senior Manager and BU Directors agreed to their designated BU ownership of devices, and their obligation to maintain processes, evidence and training; 11) created enterprise-wide documentation, which included input from Milestone 4. The new enterprise-wide documentation will be supplemented with processes to ensure compliance; 12) developed controls for the CIP-007 processes to make them repeatable and sustainable; 13) created enterprise-wide implementation evidence templates; 14) developed a Training program for new and updated documentation and implementation evidence templates. Each BU designated who is responsible for administering, maintaining, updating and tracking completion of the training program; 15) performed training; and 16) implemented new and/or updated CIP-007 documentation and controls.						
Other Factors			The Entity’s CIP-007-6 (R2) compliance history was an aggravating factor in determining the penalty.						

CONFIDENTIAL
NOC-2623

\$1,000,000

██████████ "the Entity") – ██████████

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
██████████	CIP-007-6	R3.	Medium	Severe	07/01/2016 (enforceable date of Standard when the Entity did not implement processes to deter, detect, or prevent malicious code intrusions on two Physical Access Control System (PACS) and six Electronic Access Control and/or Monitoring System (EACMS) Cyber Assets)	8/17/2018 (when the Entity completed the mitigation plan)	Audit	8/17/2018	5/8/2019
<p>Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.</p> <p>██████████ was in violation of CIP-007-6 R3.</p> <p>The Entity implemented a network system option through an intrusion detection and prevention system (IDPS) for the Cyber Assets that could not support Cyber Asset based malware prevention software. In this instance, the eight (8) Cyber Assets identified by the audit team were outside of the Electronic Security Perimeter (ESP), and thus were not available for protection by the network solution the Entity had implemented.</p> <p>The Entity confirmed that it had completed an extent of condition assessment and identified additional instances where it did not provide malware prevention protection for all Cyber Assets.</p> <p>The Entity, across its entire CIP enterprise, had ██████████. After the extent of condition assessment concluded, the Entity identified: eight (8) instances where malware prevention was absent affecting ██████████; six (6) instances where malware prevention was absent affecting ██████████ of the ██████████ PCAs, 15 instances where malware prevention was absent affecting ██████████ of the ██████████ EACMS, and two (2) instances where malware prevention was absent affecting ██████████ of the ██████████ PACS.</p> <p>The root cause for this violation was inadequate processes and a lack of controls around the deployment of malware prevention protections. Where the Entity did not utilize Cyber Asset level malware prevention at the suggestion of device vendors, the Entity also did not research or utilize a BES Cyber Systems approach for malware prevention.</p>									
Risk Assessment			<p>This violation posed a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>Specifically, the Entity’s failure to implement processes to deter, detect, or prevent malicious code on all BES Cyber Systems and related PACS and EACMS could provide the opportunity for the introduction, exposure, and propagation of malware on BES Cyber Assets within the ESP has the potential to affect the reliable operation of the BPS.</p> <p>No events or adverse consequences occurred and thus no actual harm is known to have occurred.</p>						
Mitigation			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none">1) created an inventory list of policies, standards, procedures, and work instruction documentation for malicious code prevention currently in effect for all Business Units (BU);2) developed an inventory list of all existing malicious code prevention implementation evidence templates not previously identified in milestone 1;3) determined the sustainability of existing malicious code prevention implementation evidence templates in the inventory list created in milestone 2. Decided how evidence should be structured, and how the malicious code prevention implementation evidence templates could be used to create enterprise-wide malicious code prevention evidence templates that are repeatable and sustainable;4) evaluated the inventory list created in milestone 1 of effective policies, standards, procedures, and work instruction documentation for malicious code prevention to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable;5) performed an extent of condition to confirm there is documentation based on device type for devices capable of detecting, deterring, or preventing malicious code; and, document how each device is performing (traditional AV, hardening, policies, etc.). If devices use signatures or patterns, or are not capable of malicious code prevention ensure this is documented also;6) performed an extent of condition analysis to identify possible Root Cause(s) using the inventory of documentation and devices that were identified during execution of Milestones 1, 2, and 5;7) performed a Root Cause Analysis to determine Root Cause(s) and contributing factor(s);8) developed a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the Root Cause Analysis;9) developed a technical and/or procedural solution for those devices that cannot deter, detect or prevent malicious code captured in an enterprise-wide policy document and listed the solutions and business justification, for protecting the devices;10) created enterprise-wide documentation;11) determined Roles and Responsibilities to identify ownership of devices by BU to ensure coverage;						

██████████ “the Entity”) – ██████████

CONFIDENTIAL
NOC-2623

\$1,000,000

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
██████████	CIP-007-6	R3.	Medium	Severe	07/01/2016 (enforceable date of Standard when the Entity did not implement processes to deter, detect, or prevent malicious code intrusions on two Physical Access Control System (PACS) and six Electronic Access Control and/or Monitoring System (EACMS) Cyber Assets)	8/17/2018 (when the Entity completed the mitigation plan)	Audit	8/17/2018	5/8/2019
			12) developed documented controls for the CIP-007 processes to make them repeatable and sustainable; 13) drafted a letter signed by the CIP Senior Manager and BU Directors agreeing to assigned compliance responsibilities for specific devices, including training; 14) created enterprise-wide implementation evidence templates for capturing compliance evidence; 15) developed a Training program for new and updated documentation and implementation evidence templates; 16) performed training; and 17) implemented new and/or updated CIP-007 documentation and controls.						
Other Factors			The Entity’s CIP-007-6 (R3) compliance history was an aggravating factor in determining the penalty.						

CONFIDENTIAL
NOC-2623

\$1,000,000

“the Entity”) –

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-007-6	R4. Part 4.1	Medium	Severe	07/01/2016 (enforceable date of Standard when the Entity did not implement a process to log events for identification of, and after-the-fact investigations of, Cyber Security Incidents)	8/17/2018 (when the Entity completed the mitigation plan)	Audit	8/17/2018	5/8/2019
Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.			<p>was in violation of CIP-007-6 R4.1.</p> <p>The Entity implemented a network system option through an intrusion detection and prevention system (IDPS) for the Cyber Assets that could not support Cyber Asset based malware prevention software. In this instance, the eight (8) Cyber Assets identified by the audit team were outside of the Electronic Security Perimeter (ESP), and were not available for monitoring and event logging by the network solution the Entity had implemented.</p> <p>The Entity confirmed that it had completed an extent of condition assessment and identified additional instances where the Entity did not provide event logging for all Cyber Assets.</p> <p>The Entity, across its entire CIP enterprise, had ; six (6) instances where event logging was absent affecting of the PCAs, 15 instances where event logging was absent affecting of the EACMS, and two (2) instances where event logging was absent affecting of the PACS.</p> <p>The root cause for this violation was inadequate processes and a lack of controls around the proper identification of a Cyber Assets ability to perform event logging and generation of alerts.</p>						
Risk Assessment			<p>This violation posed a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>Specifically, the Entity’s failure to monitor/log system events that are related to cyber security for its BCAs within the Electronic Security Perimeters (ESPs) could have resulted in a security breach going undetected. An undetected security breach may have compromised or rendered BES Cyber Systems inoperable, which could significantly impact the BPS.</p> <p>The risk was reduced because all the BES Cyber Assets resided within an ESP.</p> <p>No events or adverse consequences occurred and thus no actual harm is known to have occurred.</p>						
Mitigation			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none"> 1) created an inventory list of policies, standards, procedures, and work instruction documentation for security event monitoring currently in effect; 2) developed an inventory list of all existing security event monitoring implementation evidence templates not previously identified in milestone 1; 3) determined the sustainability of existing security event monitoring implementation evidence templates in the inventory list created in milestone 2. Decided how evidence should be structured, and how the security event monitoring implementation evidence templates can be used to create enterprise-wide security event monitoring evidence templates that are repeatable and sustainable; 4) evaluated the inventory list created in milestone 1 of effective policies, standards, procedures, and work instruction documentation for security event monitoring to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable; 5) performed an extent of condition to ensure there is documentation for the devices that are capable of logging and alerting on security events, to include detecting successful login attempts, failed access and login attempts, and malicious code; ensure there is documentation for the devices that can generate alerts for security events that necessitate an alert and include alerts for detected malicious code and failure of event logging; documentation for which devices are capable of retaining event logs for greater than 90 consecutive calendar days; and, documentation associated with review of logged events every 15 calendar days to identify undetected cyber security incidents for High Impact BES Cyber Systems and their associated EACMS and PCA; 6) performed an extent of condition analysis to identify possible Root Cause(s) using the inventory of documentation and devices that were identified during execution of Milestones 1, 2, and 5; 7) performed a Root Cause Analysis to determine Root Cause(s) and contributing factor(s); 8) developed a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the Root Cause Analysis; 9) created enterprise-wide documentation which will include input from Milestone 4; 10) determined Roles and Responsibilities to identify ownership of devices by BU to ensure coverage; 11) developed and documented controls for the CIP-007 processes to make them repeatable and sustainable; 						

“the Region”)

Confidential Settlement Agreement

CIP

██████████ “the Entity”) – ██████████

CONFIDENTIAL
NOC-2623

\$1,000,000

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
██████████	CIP-007-6	R4. Part 4.1	Medium	Severe	07/01/2016 (enforceable date of Standard when the Entity did not implement a process to log events for identification of, and after-the-fact investigations of, Cyber Security Incidents)	8/17/2018 (when the Entity completed the mitigation plan)	Audit	8/17/2018	5/8/2019
			12) drafted and signed a letter by the CIP Senior Manager and BU Directors agreeing to assigned compliance responsibilities for specific devices, including training; 13) created enterprise-wide implementation evidence templates for capturing compliance evidence; 14) developed training program for new and updated documentation and implementation evidence templates; 15) performed training; 16) implemented new and/or updated CIP-007 documentation and controls.						
Other Factors			The Entity’s CIP-007-6 (R4) compliance history was an aggravating factor in determining the penalty.						

CONFIDENTIAL
NOC-2623

\$1,000,000

“the Entity”) –

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-007-3a	R5. Part 5.2, Part 5.3, Part 5.7	Lower	High	12/19/2013 (when the Entity did not properly identify individuals who had authorized access to shared accounts)	12/31/2018 (when the Entity completed the mitigation plan)		12/31/2018	5/8/2019
Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.			<p>was in violation of CIP-007-6 R5. The Region later determined that the violation extended back to CIP-007-3a R5.</p> <p>The Entity did not properly identify individuals who had authorized access to shared accounts. In addition, the Entity did not file a Technical Feasibility Exception for its inability to support alerting for unsuccessful login attempts on a BES Cyber Asset (BCA), nor demonstrate its implementation of compensating and/or mitigating measures on the BCA.</p> <p>determined the Entity’s failure to track or review access to the domain accounts of (CIP-004-6 R4) was best suited to be addressed under this violation.</p> <p>The Entity completed an extent of condition assessment and identified additional instances where the Entity did not track in its internal work management tool, shared accounts and participation. The Entity had total domain administrator accounts, -shared accounts with individuals having access and non-shared individual accounts. The Entity failed to track who had access to of the domain administrator accounts. The Entity confirmed a variety of uses for the domain administrator accounts, including monitoring systems, infrastructure accounts, and accounts used to manage virtual desktops in various domains, etc. The Entity attested in the RFI response that the individuals with access to domain administrator accounts had a business need based on their job responsibilities.</p> <p>The root cause for this violation was inadequate processes and a lack of controls for system access controls, including identifying and documenting shared accounts; and, limiting the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful authentication attempts.</p>						
Risk Assessment			<p>This violation posed a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>Specifically, the Entity’s 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. 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.</p> <p>Additionally, the extent of condition assessment revealed that the Entity did not track multiple additional domain administrator accounts or the identification of individuals with access which increases the risk.</p> <p>No events or adverse consequences occurred and thus no actual harm is known to have occurred.</p>						
Mitigation			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none">1) created an inventory list of policies, standards, procedures, and work instruction documentation for system access control currently in effect;2) developed an inventory list of all existing system access control implementation evidence templates not previously identified in milestone 1;3) determined the sustainability of existing system access control implementation evidence templates in the inventory list created in milestone 2. 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;4) evaluated the inventory list created in milestone 1 of effective policies, standards, procedures, and work instruction documentation for system access control to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable;5) performed an extent of condition to evaluate system access control documentation for each device to validate if there is a method to enforce authentication of interactive user access attempts, or there is business justification documented for infeasibility (Part 5.1); documentation for enabled default or other generic account types that could not be removed, renamed or disabled is available (Part 5.2); individuals who have authorized access to shared accounts have been identified and documented (Part 5.3); records for when known default passwords are changed, or new devices are placed into production; or, documentation or vendor manuals showing that default passwords are randomly, or pseudo-randomly generated and are thereby unique to device (Part 5.4); documentation for those devices, either technically or procedurally, that support password complexity of at least 8 characters in length and 3 or more character types (Part 5.5); records showing for each device with password only authentication, a system-enforced or procedural periodicity is enforced to change passwords every 15-calendar months, or there is a documented business justification						

“the Region”)

CONFIDENTIAL
NOC-2623

\$1,000,000

“the Entity”) –

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-007-3a	R5. Part 5.2, Part 5.3, Part 5.7	Lower	High	12/19/2013 (when the Entity did not properly identify individuals who had authorized access to shared accounts)	12/31/2018 (when the Entity completed the mitigation plan)	Audit	12/31/2018	5/8/2019
			<p>for infeasibility (Part 5.6); and, documentation for which devices can limit the number of unsuccessful authentication attempts, or generate alerts after a threshold of unsuccessful authentication attempts occurs (Part 5.7);</p> <p>6) performed an extent of condition analysis to identify possible Root Cause(s);</p> <p>7) performed a Root Cause Analysis to determine Root Cause(s) and contributing factor(s);</p> <p>8) developed a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the Root Cause Analysis</p> <p>9) determined Roles and Responsibilities to identify ownership of devices by BU to ensure coverage;</p> <p>10) created enterprise-wide documentation which will include input from Milestone 4;</p> <p>11) developed and documented controls for the CIP-007 processes to make them repeatable and sustainable;</p> <p>12) drafted and signed a letter by the CIP Senior Manager and BU Directors agreeing to assigned compliance responsibilities for specific devices, including training;</p> <p>13) created enterprise-wide implementation evidence templates;</p> <p>14) reviewed and validated that all Active Directory (AD) groups in the Transmission Domain have properly assigned roles. Verified that all CIP AD roles in the Access Provisioning System (APS) have a corresponding access management role, that all Transmission CIP AD access management roles are found in APS, and that all Transmission AD administrators have a corresponding access management role;</p> <p>15) moved all Transmission Active Directory (AD) access from Access Provisioning System (APS) to Enterprise Access Management System (EAMS);</p> <p>16) identified how the Access Control Lists (ACL) are determined across the various platform types;</p> <p>17) developed a training program for new and updated documentation and implementation evidence templates;</p> <p>18) performed training;</p> <p>19) performed an extent of condition by identifying all CIP non-Windows devices, and mapping all roles from the CIP non-Windows device to the access management system roles in EAMS. Verified that access to CIP non-Windows devices is granted through access management roles. Created new roles if discrepancies are identified. Assigned appropriate personnel to any new role once confirmed they are eligible and have a business need;</p> <p>20) created a standardized enterprise-wide access matrix template with clearly defined roles;</p> <p>21) implemented countermeasures and execute updated CIP-007 documents and controls;</p> <p>22) developed a mechanism for extracting and comparing the access management tool's users and roles to target system's Access Control List (ACL);</p> <p>23) performed an Extent of Condition (extent of condition) by identifying all CIP Windows devices, and mapping all roles from the CIP Windows device to the access management system roles in EAMS. Created new roles if discrepancies are identified. Assigned appropriate personnel to any new role once confirmed they are eligible and have a business need;</p> <p>24) cleaned-up and restructure roles; and</p> <p>25) created a new enterprise-wide access matrix, and populate with roles.</p>						
Other Factors			The Entity's CIP-007-6 (R5) compliance history was an aggravating factor in determining the penalty.						

CONFIDENTIAL
NOC-2623

\$1,000,000

██████████ “the Entity”) – ██████████

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
██████████	CIP-010-2	R2.	Medium	Severe	07/01/2016 (enforceable date of Standard when the Entity did not have documented processes for investigating detected unauthorized changes to baseline configurations of its BES Cyber Assets, as required)	02/28/2018 (when the Entity completed the mitigation plan)	Audit	02/28/2018	10/25/2018
Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.			██████████ was in violation of CIP-010-2 R2. The Entity did not have documented processes for investigating detected unauthorized changes to baseline configurations of its BES Cyber Assets, as required. The Entity confirmed that it had completed an extent of condition assessment. The Entity identified six configuration change management processes for high impact Bulk Electric System Cyber Systems (BCSs) which lacked detailed procedural steps. The root cause for this violation was a lack of documented steps for documenting or investigating detected unauthorized changes.						
Risk Assessment			This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Specifically, the Entity’s failure to have detailed work instructions could leave a responding technician unsure of what steps or actions should be taken in response to a detected unauthorized change, creating an opportunity for key, time sensitive steps to be omitted resulting in an unstable or vulnerable energy management system thereby placing the reliability of the BPS at risk. The risk was reduced because the Entity did have a process in place, but it lacked specifics on what actions to take when investigating detected unauthorized changes. No events or adverse consequences occurred and thus no actual harm is known to have occurred.						
Mitigation			To mitigate this violation, the Entity: 1) performed an extent of condition analysis to identify all procedures for High Impact BCS within the Responsible Entity that require enhancements to include the process for documenting and investigating detected unauthorized changes; 2) developed narrative for enhancements; 3) incorporated the enhancements developed in Milestone No. 2, including the creation of new controls, into the CIP-010 Procedures for High Impact BCS. Ensured linkages are established to other relevant Cyber Security Policies and Procedures. 4) obtained and documented the required approvals and sign-offs of revised documentation before training; 5) scheduled and administered training to those individuals within the Responsible Entity who perform the tasks covered by the procedures. Training will be designed to sustain ongoing content updates, tracking and delivery; 6) communicated and disseminated documentation enterprise-wide by notifying impacted personnel of updates to documentation; and 7) corrected for any deficiencies found while completing the previous milestones.						
Other Factors									

CONFIDENTIAL
NOC-2623

\$1,000,000

██████████ "the Entity") – ██████████

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
██████████	CIP-011-2	R1.	Medium	Severe	07/01/2016 (enforceable date of Standard when the Entity did not properly identify a storage area network Cyber Asset used to store security configurations)	04/25/2018 (when the Entity completed the mitigation plan)	Audit	4/25/2018	5/8/2019
Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.			██████████ was in violation of CIP-011-2 R1. The Entity did not properly identify a storage area network Cyber Asset used to store security configurations of its BES Cyber Assets (BCA) as a BES Cyber System Information (BCSI) storage location. The extent of condition assessment did not reveal any additional instances. The root cause for this violation was lack of a documented methodology that included a detailed assessment to account for all locations that may contain BCSI.						
Risk Assessment			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Specifically, the Entity's failure to properly identify and document a BCSI repository could have permitted critical information to be stored on more easily accessible and less protected systems and allowed unauthorized disclosure of BCSI Information. This disclosure could have allowed an intruder to make use of such information in a Cyber attack and could increase the number of attack vectors to BES Cyber Systems. The risk was reduced because the server was within a secured cabinet that had card-reader controlled access and within a partitioned section of secured network. In addition, the server was afforded protections as a BCA even though it was not classified as such and access was restricted to five (5) individuals with completed personnel risk assessments who were all properly trained. No events or adverse consequences occurred and thus no actual harm is known to have occurred.						
Mitigation			To mitigate this violation, the Entity: 1) determined if there is a related access role, for the cited BES Cyber System Information (BCSI) Storage Location, in the ██████████ for the storage location cited, and document the evidence if the role exists in ██████████. If there is no access role in ██████████ for this location, create a role to ensure the location is properly identified as a BCSI Storage Location with access controls. Performed a risk assessment to fully understand the BES risk; 2) performed an extent of condition analysis to (1) Identify any BCSI Storage Locations that have not been properly identified; and, (2) Identify and document the existence of any unknown additional root causes; 3) performed Root Cause Analysis to (1) Identify possible root cause(s) for the storage location not being properly identified; and, (2) Verify the root cause(s) by identifying and validating the contributing factors 4) developed list of countermeasures leveraging results from the Root Cause Analysis; and, develop 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); 5) addressed any extent of condition findings by: (1) Creating any necessary additional ██████████ access roles for any BCSI Storage Location(s) identified; (2) Assign access to any new storage locations identified; and, (3) Properly classify and label the electronic and/or physical documents for any new storage locations identified; 6) implemented countermeasures for enterprise-wide methodology to identify BCSI; 7) developed and delivered training; and 8) communicated and disseminated newly revised IPP documentation enterprise-wide.						
Other Factors									

CONFIDENTIAL
NOC-2623

\$1,000,000

“the Entity”) –

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	CIP-005-3a	R2. R2.1, R2.2.	Medium	Severe	11/05/2011 (the Entity did not have sufficient documentation to demonstrate ports and services required)	12/14/2015 (when the Entity corrected the unnecessary broad ranges of both IP subnets and ports issues, updated the documentation to reflect new changes.)	Audit	12/14/2015	10/26/2016
Description of the Violation (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, or confirmed violation.) The Entity neither admits nor denies any of these statements or that they constitute a violation.			<p>was in violation of CIP-005-3a R2.1 and R2.2.</p> <p>The Entity documentation was insufficient to demonstrate that it uses an access control model such that explicit access permissions are specified. In addition, the the Entity documentation was insufficient to demonstrate that it enabled only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter; and that the Entity documented individually or by specified grouping, the configuration of those ports and services.</p> <p>Specifically, the Entity's documentation illustrates permit statements that include the entire range of ports from as well as all devices in a subnet using masking. The Entity's supplied documentation for the justification of the allowed ports were actually the results of a CVA that show the open ports discovered during an assessment and did not demonstrate why the entire range of ports from were allowed at the access point. Additionally, the entire range of IP addresses in the subnet mask used could not substantiated as explicit given many of the addresses were not used.</p>						
Risk Assessment			<p>This violation posed a serious or substantial risk to the reliability of the bulk power system.</p> <p>Failure to use explicit permissions does not limit network communications traffic to specific devices and in addition not evaluating ports/services needed for operations or monitoring can potentially allow for unauthorized traffic.</p>						
Mitigation			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none"> 1) created an inventory list of policies, standards, procedures, and work instruction documentation for security event monitoring currently in effect; 2) developed an inventory list of all existing security event monitoring implementation evidence templates not previously identified in milestone 1; 3) determined the sustainability of existing security event monitoring implementation evidence templates in the inventory list created in milestone 2. Decided how evidence should be structured, and how the security event monitoring implementation evidence templates can be used to create enterprise-wide security event monitoring evidence templates that are repeatable and sustainable; 4) evaluated the inventory list created in milestone 1 of effective policies, standards, procedures, and work instruction documentation for security event monitoring to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable; 5) performed an extent of condition assessment to ensure there is documentation for the devices that are capable of logging and alerting on security events, to include detecting successful login attempts, failed access and login attempts, and malicious code; ensure there is documentation for the devices that can generate alerts for security events that necessitate an alert and include alerts for detected malicious code and failure of event logging; documentation for which devices are capable of retaining event logs for greater than 90 consecutive calendar days; and, documentation associated with review of logged events every 15 calendar days to identify undetected cyber security incidents for High Impact BES Cyber Systems and their associated EACMS and PCA; 6) performed an extent of condition analysis to identify possible Root Cause(s) using the inventory of documentation and devices that were identified during execution of Milestones 1, 2, and 5; 7) performed a Root Cause Analysis to determine Root Cause(s) and contributing factor(s); 8) developed a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the Root Cause Analysis; 9) created enterprise-wide documentation which will include input from Milestone 4; 10) determined Roles and Responsibilities to identify ownership of devices by BU to ensure coverage; 11) developed and documented controls for the CIP-007 processes to make them repeatable and sustainable; 12) drafted and signed a letter by the CIP Senior Manager and BU Directors agreeing to assigned compliance responsibilities for specific devices, including training; 13) created enterprise-wide implementation evidence templates for capturing compliance evidence; 14) developed Training program for new and updated documentation and implementation evidence templates; 15) performed training; and 16) implemented new and/or updated CIP-007 documentation and controls. 						
Other Factors			The Entity's CIP-005-3a (R2) compliance history was an aggravating factor in determining the penalty.						

“the Region”)

Confidential Settlement Agreement

CIP

Attachment 4

- 4a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-004-6 R3 submitted February 14, 2018
- 4b. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R3 submitted February 14, 2018
- 4c. The Region's Verification of Mitigation Plan Completion for CIP-004-6 R3 dated October 24, 2018

A previous version of this Mitigation Plan exists

This item was signed by [REDACTED] on 2/14/2018

This item was marked ready for signature by [REDACTED] on 2/14/2018

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name:

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard:

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R3.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

The possible violation relates to the Responsible Entity's procedure for verifying Personnel Risk Assessments (PRAs) by Contractors with authorized access to BES Cyber Systems ("CIP access"). During the audit, as a condition of obtaining CIP access, the Responsible Entity relied on signed affidavits from Contractors ensuring the completion of a legitimate seven-year criminal background check covering all areas required by NERC. [REDACTED] faulted this process by noting that "the company did not verify the performance of attestations associated with PRAs performed by contractors, as required" (p.10). In addition, the audit team reported that the Responsible Entity was unable to provide a PRA affidavit for one Contractor with CIP access from its sample population (p.11).

A preliminary root cause analysis highlighted two main reasons for the possible violation finding. First, the procedure for verifying Contractor PRAs relied solely on signed affidavits from Contractors without validation of the full scope covered in performance of the seven-year background check. Second, the Responsible Entity failed to adequately implement procedures for maintaining signed affidavits from Contractors seeking to obtain or retain CIP access. An insufficient procedure, combined with inadequate implementation led to the possible violation that will be remediated by this Mitigation Plan.

[Attachments \(\)](#)

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this Mitigation Plan:

The system control center assets are utilized by the Responsible Entity to perform functions for the reliable operation of the BES. Given the importance of this function to the reliable operation of the BES, the Responsible Entity prioritized verification of Contractors with CIP access to system control centers while developing and finalizing this Mitigation Plan.

[Attachments \(\)](#)

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

0: Preliminary Root Cause Analysis. During the time period starting on December 7, 2016 through February 1, 2017, representatives from [REDACTED]

met to assess the reason(s) for the possible violation. During five (5) scheduled meetings, the team identified the gaps associated with the existing PRA process for Contractors and Service vendors and collaboratively developed a Mitigation Plan to remediate. Completed by February 1, 2017.

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

1: Develop an enterprise wide Personnel Risk Assessment (PRA) Procedure for verifying Contractor and Service vendor background checks. Additionally review and revise, as needed, program documentation associated with PRAs for Contractors and Service vendors. The enterprise-wide PRA Procedure for verifying Contractor and Service vendor background checks will include: (1) How Business Units (BUs) will verify PRAs for Contractors, Service vendors, and subcontractors of Contractors and Service vendors that have a master service agreement or contract; and, (2) Requiring that both the affidavit and details of the PRA evaluation for Contractors, Service vendors, and subcontractors be retained. Revisions to PRA Procedure will include: (1) Execution of review and completion of PRA evaluation template; (2) Review with legal for any questionable findings on PRA; (3) Destruction of PRA after contents are documented in template; and, (4) Filing affidavit and evaluation template as evidence. Completed by August 31, 2017.

2: Develop and document controls to ensure Contractor and Service vendor PRA process will be implemented as documented. Operational BUs will develop controls to ensure documented process steps are followed; and, the controls will be incorporated into the newly revised enterprise-wide PRA Procedure for verifying Contractor and Service vendor background checks. Completed by August 31, 2017.

3: Develop a training program for Contractor and Service vendor PRAs. Training program will include training materials on revised and enhanced process for handling Contractor PRAs, delivery of initial training course to Operational BU Representatives who are responsible for granting unescorted physical or electronic access to BES Cyber Systems, and controls for ensuring evaluation of PRAs for Contractors and Service vendors. Completed by October 31, 2017.

4: Implement updated PRA Procedure. Operational BUs will implement updated process and controls for Contractor and Service vendor PRAs. Completed by November 15, 2017.

5: Extent of Condition: Based on the newly revised and implemented procedure for Contractor and Service vendor PRAs, conduct an Extent of Condition analysis with goal of verifying that 100% of PRAs have been evaluated for Contractors and Service vendors according to contractual Supplemental Terms & Conditions (T&Cs). The Business Unit Contract Coordinator (BUCC), or an assigned approver for each Operational BU, with Contractors and Service vendors that have been granted CIP access, or have the possibility of being granted CIP access, shall: (1) Identify all Contractors and Service vendors with CIP access or the possibility of being granted CIP access since April 1, 2016 through provisions in the Supplemental T&Cs that require copies of PRAs from Contractors, Service vendors, and subcontractors of the Contractors or Service vendors; (2) Evaluate the PRAs by completing the template; and, (3) Retain a copy of the affidavit and evaluation template for each Contractor and Service vendor. If a copy of the Contractor or Service vendor's PRA is not provided for evaluation, or the PRA fails to meet the requirements according to the Supplemental T&Cs, the Contractor's or Service vendor's access will be revoked within 24-hours from the date and time of discovery. Integrated Supply Chain and the BU Vendor Representative will be advised that the Contractor or Service vendor is not in compliance with the T&Cs and appropriate action will be taken to revoke access; and, (2) Results of the PRA evaluation for all Contractors and Service vendors will be documented. Completed by December 31, 2017.

6: Add "Training" section to the PRA procedure that will define who will be required to take training on the PRA process and why, as well as the periodicity for any refresher training. Team will define both initial and refresher training requirements and document in the PRA procedure. This training will be incorporated into the Enterprise-wide training program that will be covered under Recommendation #2. To be completed by February 28, 2018.

Attachments ()

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

2/28/2018

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

Conduct an Extent of Condition

Milestone Completed (Due: 12/31/2017 and Completed 12/29/2017)

Based on the newly revised and implemented procedure for Contractor and Service vendor PRAs, conduct an Extent of Condition analysis with goal of verifying that 100% of PRAs have been evaluated for Contractors and Service vendors according to contractual Supplemental Terms & Conditions (T&Cs). The Business Unit Contract Coordinator (BUCC), or an assigned approver for each Operational BU, with Contractors and Service vendors that have been granted CIP access, or have the possibility of being granted CIP access, shall: (1) Identify all Contractors and Service vendors with CIP access or the possibility of being granted CIP access since April 1, 2016 through provisions in the Supplemental T&Cs that require copies of PRAs from Contractors, Service vendors, and subcontractors of the Contractors or Service vendors; (2) Evaluate the PRAs by completing the template; and, (3) Retain a copy of the affidavit and evaluation template for each Contractor and Service vendor. If a copy of the Contractor or Service vendor's PRA is not provided for evaluation, or the PRA fails to meet the requirements according to the Supplemental T&Cs, the Contractor's or Service vendor's access will be revoked within 24-hours from the date and time of discovery. Integrated Supply Chain and the BU Vendor Representative will be advised that the Contractor or Service vendor is not in compliance with the T&Cs and appropriate action will be taken to revoke access; and, (2) Results of the PRA evaluation for all Contractors and Service vendors will be documented.

PRA Training Program

Milestone Pending (Due: 2/28/2018)

Add "Training" section to the PRA procedure that will define who will be required to take training on the PRA process and why, as well as the periodicity for any refresher training. Team will define both initial and refresher training requirements and document in the PRA procedure. This training will be incorporated into the Enterprise-wide training program that will be covered under Recommendation #2.

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

The possible violation finding raised awareness that individuals working for third-party contractors could obtain CIP access without an appropriate level of risk assessment. Due to the seriousness of this security risk, the Responsible Entity will verify the sufficiency of the PRAs performed for all Contractors and Service vendors with CIP access. This work will culminate with the completion of an Extent of Condition analysis in Milestone 5 by December 31, 2017. Following the Extent of Condition analysis, any identified Contractor or Service vendor in which the PRA has not been assessed will no longer have CIP access. Where possible, the Responsible Entity prioritized verification of Contractors and Service vendors with CIP access to system control centers while implementing the Mitigation Plan.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

After completion of all milestone activities, the Responsible Entity will have implemented a more comprehensive program for managing PRAs, including specifically evaluating what information was collected in the performance of a background check for all Contractors and Service vendors. There will be a training program in place to ensure Personnel who are responsible for Contractors and or Service vendors understand the PRA evaluation that must be performed before the Contractor or Service vendor is granted CIP access. The sufficiency of background checks performed for all Contractors and Service vendors will have been validated prior to obtaining CIP access.

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am [REDACTED]
 - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
 - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
 - I have read and am familiar with the contents of this Mitigation Plan
 - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED], please contact the [REDACTED] department to determine your assigned SPOC at:

[REDACTED]

[REDACTED]

[REDACTED]

A previous version of this Mitigation Plan exists

This item was signed by [REDACTED] on 2/14/2018

This item was marked ready for signature by [REDACTED] on 2/14/2018

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name:

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard:

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R3.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

The possible violation relates to the Responsible Entity's procedure for verifying Personnel Risk Assessments (PRAs) by Contractors with authorized access to BES Cyber Systems ("CIP access"). During the audit, as a condition of obtaining CIP access, the Responsible Entity relied on signed affidavits from Contractors ensuring the completion of a legitimate seven-year criminal background check covering all areas required by NERC. [REDACTED] faulted this process by noting that "the company did not verify the performance of attestations associated with PRAs performed by contractors, as required" (p.10). In addition, the audit team reported that the Responsible Entity was unable to provide a PRA affidavit for one Contractor with CIP access from its sample population (p.11).

A preliminary root cause analysis highlighted two main reasons for the possible violation finding. First, the procedure for verifying Contractor PRAs relied solely on signed affidavits from Contractors without validation of the full scope covered in performance of the seven-year background check. Second, the Responsible Entity failed to adequately implement procedures for maintaining signed affidavits from Contractors seeking to obtain or retain CIP access. An insufficient procedure, combined with inadequate implementation led to the possible violation that will be remediated by this Mitigation Plan.

[Attachments \(\)](#)

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this Mitigation Plan:

The system control center assets are utilized by the Responsible Entity to perform functions for the reliable operation of the BES. Given the importance of this function to the reliable operation of the BES, the Responsible Entity prioritized verification of Contractors with CIP access to system control centers while developing and finalizing this Mitigation Plan.

[Attachments \(\)](#)

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

0: Preliminary Root Cause Analysis. During the time period starting on December 7, 2016 through February 1, 2017, representatives from [REDACTED]

met to assess the reason(s) for the possible violation. During five (5) scheduled meetings, the team identified the gaps associated with the existing PRA process for Contractors and Service vendors and collaboratively developed a Mitigation Plan to remediate. Completed by February 1, 2017.

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

1: Develop an enterprise wide Personnel Risk Assessment (PRA) Procedure for verifying Contractor and Service vendor background checks. Additionally review and revise, as needed, program documentation associated with PRAs for Contractors and Service vendors. The enterprise-wide PRA Procedure for verifying Contractor and Service vendor background checks will include: (1) How Business Units (BUs) will verify PRAs for Contractors, Service vendors, and subcontractors of Contractors and Service vendors that have a master service agreement or contract; and, (2) Requiring that both the affidavit and details of the PRA evaluation for Contractors, Service vendors, and subcontractors be retained. Revisions to PRA Procedure will include: (1) Execution of review and completion of PRA evaluation template; (2) Review with legal for any questionable findings on PRA; (3) Destruction of PRA after contents are documented in template; and, (4) Filing affidavit and evaluation template as evidence. Completed by August 31, 2017.

2: Develop and document controls to ensure Contractor and Service vendor PRA process will be implemented as documented. Operational BUs will develop controls to ensure documented process steps are followed; and, the controls will be incorporated into the newly revised enterprise-wide PRA Procedure for verifying Contractor and Service vendor background checks. Completed by August 31, 2017.

3: Develop a training program for Contractor and Service vendor PRAs. Training program will include training materials on revised and enhanced process for handling Contractor PRAs, delivery of initial training course to Operational BU Representatives who are responsible for granting unescorted physical or electronic access to BES Cyber Systems, and controls for ensuring evaluation of PRAs for Contractors and Service vendors. Completed by October 31, 2017.

4: Implement updated PRA Procedure. Operational BUs will implement updated process and controls for Contractor and Service vendor PRAs. Completed by November 15, 2017.

5: Extent of Condition: Based on the newly revised and implemented procedure for Contractor and Service vendor PRAs, conduct an Extent of Condition analysis with goal of verifying that 100% of PRAs have been evaluated for Contractors and Service vendors according to contractual Supplemental Terms & Conditions (T&Cs). The Business Unit Contract Coordinator (BUCC), or an assigned approver for each Operational BU, with Contractors and Service vendors that have been granted CIP access, or have the possibility of being granted CIP access, shall: (1) Identify all Contractors and Service vendors with CIP access or the possibility of being granted CIP access since April 1, 2016 through provisions in the Supplemental T&Cs that require copies of PRAs from Contractors, Service vendors, and subcontractors of the Contractors or Service vendors; (2) Evaluate the PRAs by completing the template; and, (3) Retain a copy of the affidavit and evaluation template for each Contractor and Service vendor. If a copy of the Contractor or Service vendor's PRA is not provided for evaluation, or the PRA fails to meet the requirements according to the Supplemental T&Cs, the Contractor's or Service vendor's access will be revoked within 24-hours from the date and time of discovery. Integrated Supply Chain and the BU Vendor Representative will be advised that the Contractor or Service vendor is not in compliance with the T&Cs and appropriate action will be taken to revoke access; and, (2) Results of the PRA evaluation for all Contractors and Service vendors will be documented. Completed by December 31, 2017.

6: Add "Training" section to the PRA procedure that will define who will be required to take training on the PRA process and why, as well as the periodicity for any refresher training. Team will define both initial and refresher training requirements and document in the PRA procedure. This training will be incorporated into the Enterprise-wide training program that will be covered under Recommendation #2. To be completed by February 28, 2018.

Attachments ()

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

2/28/2018

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

Conduct an Extent of Condition

Milestone Completed (Due: 12/31/2017 and Completed 12/29/2017)

Based on the newly revised and implemented procedure for Contractor and Service vendor PRAs, conduct an Extent of Condition analysis with goal of verifying that 100% of PRAs have been evaluated for Contractors and Service vendors according to contractual Supplemental Terms & Conditions (T&Cs). The Business Unit Contract Coordinator (BUCC), or an assigned approver for each Operational BU, with Contractors and Service vendors that have been granted CIP access, or have the possibility of being granted CIP access, shall: (1) Identify all Contractors and Service vendors with CIP access or the possibility of being granted CIP access since April 1, 2016 through provisions in the Supplemental T&Cs that require copies of PRAs from Contractors, Service vendors, and subcontractors of the Contractors or Service vendors; (2) Evaluate the PRAs by completing the template; and, (3) Retain a copy of the affidavit and evaluation template for each Contractor and Service vendor. If a copy of the Contractor or Service vendor's PRA is not provided for evaluation, or the PRA fails to meet the requirements according to the Supplemental T&Cs, the Contractor's or Service vendor's access will be revoked within 24-hours from the date and time of discovery. Integrated Supply Chain and the BU Vendor Representative will be advised that the Contractor or Service vendor is not in compliance with the T&Cs and appropriate action will be taken to revoke access; and, (2) Results of the PRA evaluation for all Contractors and Service vendors will be documented.

PRA Training Program

Milestone Pending (Due: 2/28/2018)

Add "Training" section to the PRA procedure that will define who will be required to take training on the PRA process and why, as well as the periodicity for any refresher training. Team will define both initial and refresher training requirements and document in the PRA procedure. This training will be incorporated into the Enterprise-wide training program that will be covered under Recommendation #2.

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

The possible violation finding raised awareness that individuals working for third-party contractors could obtain CIP access without an appropriate level of risk assessment. Due to the seriousness of this security risk, the Responsible Entity will verify the sufficiency of the PRAs performed for all Contractors and Service vendors with CIP access. This work will culminate with the completion of an Extent of Condition analysis in Milestone 5 by December 31, 2017. Following the Extent of Condition analysis, any identified Contractor or Service vendor in which the PRA has not been assessed will no longer have CIP access. Where possible, the Responsible Entity prioritized verification of Contractors and Service vendors with CIP access to system control centers while implementing the Mitigation Plan.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

After completion of all milestone activities, the Responsible Entity will have implemented a more comprehensive program for managing PRAs, including specifically evaluating what information was collected in the performance of a background check for all Contractors and Service vendors. There will be a training program in place to ensure Personnel who are responsible for Contractors and or Service vendors understand the PRA evaluation that must be performed before the Contractor or Service vendor is granted CIP access. The sufficiency of background checks performed for all Contractors and Service vendors will have been validated prior to obtaining CIP access.

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am [REDACTED]
 - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
 - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
 - I have read and am familiar with the contents of this Mitigation Plan
 - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED], please contact the [REDACTED] department to determine your assigned SPOC at:

[REDACTED]

[REDACTED]

[REDACTED]

VIA Secure Folder and E-MAIL

October 24, 2018

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED] (CIP-004-6 R3)

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-004-6 R3	February 14, 2018

After review for completion on **October 24, 2018**, [REDACTED] staff finds that [REDACTED]
has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this
mitigation plan.

If you have any questions, please feel free to contact [REDACTED].

[REDACTED]

[REDACTED]

Attachment 5

- 5a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-004-6 R4 submitted June 19, 2018
- 5b. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R4 submitted July 20, 2018
- 5c. The Region's Verification of Mitigation Plan Completion for CIP-004-6 R4 dated October 24, 2018

This item was signed by [REDACTED] on 6/19/2018

This item was marked ready for signature by [REDACTED] on 6/19/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation IDs	Date Submitted	Status	Type	Revision Number
CIP-004-6 R4.	[REDACTED]	[REDACTED]	06/19/2018	Region reviewing Mitigation Plan	Formal	

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name:

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard:

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R4.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

[REDACTED] the Responsible Entity "did not properly track access authorizations of its domain administrator accounts. In addition, [Responsible Entity] 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, [Responsible Entity] was not in compliance with the CIP Reliability Standard CIP-004-6 Requirement R4. In addition, as [Responsible Entity's] programs at issue are used for or related to the [Reliability Coordinator] function, [Reliability Coordinator] was not in compliance with the CIP Reliability Standard CIP-004-6 Requirement R4." (p.11)

Attachments ()

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this Mitigation Plan:

The Responsible Entity identified four unrelated issues as a result of the audit. They were: (1) The Responsible Entity failed to track domain administrator accounts in its [REDACTED]. Thus, authorized access to domain accounts was not being validated by the automated verification process, which tracks a user's business need, training, and the status of their Personnel Risk Assessment (PRA). (2) One individual, without authorized unescorted physical access, temporarily had in their possession a "physical" key to a Physical Security Perimeter (PSP). They were to deliver the key to an individual that had authorized unescorted physical access. There was not a process in place that covered the proper handling of "physical" keys. (3) In an effort to centralize the "physical" key management process, a [REDACTED] key custodian had access to "physical" keys, but did not have authorized unescorted physical access to the PSPs. The custodian did not have a business need to use the "physical" keys for access to the PSPs, but they were responsible for storing and issuing the "physical" keys to those who did have a business need to use the "physical" key and authorized unescorted physical access to the PSPs. Procedures did not include language covering "physical" key authorizations for each individual in possession of a "physical" key. (4) [REDACTED] also did not cover in its existing [REDACTED] procedure instructions for ensuring that "physical" keys are only distributed to individuals with authorized unescorted physical access to PSPs.

Attachments ()

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing, or has completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

- 1: Create a new role in the [REDACTED] for an [REDACTED] within the [REDACTED] domain. Completed by September 26, 2016.
- 2: Remove "physical" keys from the [REDACTED] custodian who does not have authorized unescorted physical access to the PSPs. Document by area, the transfer of "physical" keys to the [REDACTED] in the area "physical" key control log. Compare [REDACTED] "physical" key control logs to [REDACTED] custodian "physical" key control log to ensure all "physical" keys are logged. Completed by March 27, 2017.
- 3: Validate [REDACTED] "physical" key custodians, their "physical" key custodian roles, and the "physical" key distribution process [REDACTED] re roles are created to manage [REDACTED] "physical" key custodians have authorized unescorted physical access to the PSPs under their responsibility. Revise "physical" key authorizations and "physical" key distribution process. Completed by June 16, 2017.
- 4: Create separate roles in [REDACTED] for (1) CIP physical asset access; and (2) CIP Cyber Asset access. Verify that no CIP access role in [REDACTED] provides both physical and Cyber Asset access. Completed by September 14, 2017.
- 5: Update the "physical" key distribution procedure for [REDACTED] to require [REDACTED] to verify that an individual has authorized unescorted access to a PSP before issuing a "physical" key. [REDACTED] substation [REDACTED] responsible for the protection and distribution of "physical" keys will be trained on the updated "physical" key distribution procedure. Completed by September 20, 2017.
- 6: Perform an Extent of Condition (EOC) to validate the [REDACTED] and [REDACTED] "physical" key custodian process ensures that only individuals with authorized unescorted physical access are responsible for [REDACTED] and issuing "physical" keys. EOC will include: (1) Using the respective "physical" key inventory list(s), validate that all "physical" keys and assigned "physical" key custodians for [REDACTED] and [REDACTED] are recorded. (2) Confirm that all "physical" keys are assigned to a "physical" key custodian that has authorized unescorted physical access. (3) Validate that the PGD and PD substations' "physical" key [REDACTED] "physical" keys are only maintained by authorized "physical" key custodians who have the appropriately assigned [REDACTED] "physical" key custodian role. (4) Revise or create documentation, if necessary, to support the "physical" key authorization and distribution process. (5) Notify [REDACTED] of any additional [REDACTED] by [REDACTED]
- 7: Hold a training session on management's expectations, responsibilities, and the updated procedure for managing access to "physical" keys with [REDACTED] that are assigned [REDACTED] roles. Completed by October 25, 2017.
- 8: Verify that [REDACTED] roles exist for [REDACTED] in [REDACTED] for those responsible for managing "physical" keys. Create [REDACTED] roles for "physical" keys in [REDACTED] and report any additional discrepancies identified during verification to the [REDACTED]. Completed by November 13, 2017.
- 9: Train "physical" key custodians on the responsibilities associated with [REDACTED] access verification process for controlling "physical" keys. Completed by November 13, 2017.
- 10: Revise and implement the [REDACTED] "physical" key control procedure used to manage [REDACTED] owned Physical Security Perimeters (PSPs) and High Impact Control Centers. Document the approved "physical" key custodians. Revise the IT "physical" key distribution process to confirm that it includes a statement that "physical" keys are only provided to individuals with authorized unescorted physical access to PSPs and are assigned the "physical" key custodian role in [REDACTED]. Revise documentation for "physical" key authorizations and distribution to include control processes. Completed by November 20, 2017.
- 11: Remediate any discrepancies found in the Extent of Condition performed in milestone 6. Completed by November 27, 2017.
- 12: Review initial root causes identified during the development of Mitigation Plan, and verify that corrective measures have been implemented for root causes and contributing factors. Document if additional root causes or contributing factors were found through implementation of corrective measures; and, document any additional preventive or detective controls identified that need to be implemented. Completed by December 4, 2017.
- 13: Create an enterprise-wide "physical" key management process for Medium and High Impact Physical Security Perimeters (PSPs). Using the documentation of the individual [REDACTED] for the distribution and control of "physical" keys, create enterprise-wide process documentation to include authorizations. Completed by January 26, 2018.
- 14: Train and implement the newly created enterprise-wide "physical" key distribution documentation. Train "physical" key custodians on the new enterprise-wide "physical" key distribution process. Implement the new enterprise-wide "physical" key distribution process and retire the individual [REDACTED] processes. Completed by March 8, 2018.

Attachments ()

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

3/8/2018

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

No Milestones Defined

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

The Responsible Entity has [REDACTED] to the [REDACTED] plan that is [REDACTED] distinct issues underlying the possible violation (PV) in the Final Audit Report. The distinct categories remediated by this Mitigation Plan are effectively tracking access authorizations to the domain administrator accounts in the [REDACTED] and tightening the control and distribution of "physical" keys. For the following reasons, the Responsible Entity believes that the [REDACTED] only minimal risk to the reliability of the BES during execution of this multi-faceted Mitigation Plan.

Abatement of any putative risk to the reliability of the BES began August 26, 2016 (see Milestone 1), shortly after [REDACTED]. An [REDACTED] role did not exist for the [REDACTED] group [REDACTED]. As part of an audit data request, an [REDACTED] role was created and assigned to the individuals who were members of [REDACTED] Personnel Risk Assessment (PRA) was on file, and the individual had completed the required training. An [REDACTED] role was also established for the [REDACTED] account, in which users shared a password to the same account), to manage individual authorizations to the password of the shared account. Thus by September 26, 2016, the Responsible Entity was tracking who had assigned roles to the [REDACTED] and shared accounts in [REDACTED]

The audit [REDACTED] identified an individual who was not approved for unescorted physical access, since they had not completed the CIP training, but was found to be in possession of "physical" keys to the Medium Impact Substations. There was however a PRA on file for this individual. The individual was simply the custodian of the "physical" keys, who tracked the issuance of "physical" [REDACTED] unescorted [REDACTED] the Entity's Substations.

During the course of the audit, the Responsible Entity began evaluating the auditors' questions about the management of "physical keys", and based upon this appraisal, the Responsible Entity decided to remediate the issues raised concerning the management of "physical" keys. By March 27, 2017, the [REDACTED] custodian no longer had control of "physical" keys; and, the control of [REDACTED] d to [REDACTED] with responsibilities for the seven (7)

areas constituting the Responsible Entity's service territory, (see Milestone 2). Each [REDACTED] is now the custodian of the "physical" keys and has authorized unescorted access to the sites where the "physical" keys are used for access.

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

[REDACTED] another instance where an individual did not have authorized unescorted access to the Back-up Control Center. This observance was related to the transfer of a "physical" key during the summer of 2016 from the primary Control Center to [REDACTED] Control Center. [REDACTED] An [REDACTED] of the Responsible Entity, realized that the "physical" key to the Back-up Control Center was being stored at the Primary Control Center and decided that it would be prudent to have the "physical" key relocated to the Back-up Control Center. This would allow the "physical" key to the Back-up Control Center to be readily accessible in the event it was needed for access to the PSP, (in the case of the electronic P, [REDACTED])

In order to effectuate the transfer, the [REDACTED] asked an [REDACTED] to deliver the "physical" key to the Responsible Entity's corporate offices in [REDACTED]. The "Override Key Log" accurately reflects the sign-out of the "physical" key by [REDACTED] on July 6, 2016. The [REDACTED] delivered the "physical" key to the [REDACTED], who then transferred the "physical" key to the [REDACTED], an employee who has authorized unescorted access to the Back-up Control Center. The [REDACTED] who generally travels to the Back-up Control Center one day each month, then transported the key to the Back-up Control Center and logged it in on August 8, 2016.

Although the [REDACTED] and [REDACTED] did not have authorized unescorted access to the Back-up Control Center at the time of the "physical" key transfer, both were employees who had PRAs on file. Additionally, the [REDACTED] was officially granted authorized unescorted access on September 27, 2016; and, the [REDACTED] was officially granted authorized unescorted access on September 26, 2016 to the Back-up Control Center. Thus, there was minimal risk associated with the transfer of the "physical" key.

In an abundance of caution, and due to their widely dispersed locations, the Responsible Entity decided to re-core and re-key all PSPs at Medium Impact Substations in the highly unlikely event that a "physical" key had been duplicated, or stolen by an individual with nefarious intentions. As of July 14, 2017, all locks at the Medium Impact Substations had been re-cored and re-keyed. Presently, if anyone attempts to access a facility with a "physical" key rather than through the PACS, which is the adopted security protocol for physical access, [REDACTED] would immediately be notified, and security personnel or local law enforcement would immediately respond.

As of February 9, 2018, all milestone activities designed specifically for the management of "physical" keys had been completed, thereby resolving any risk attributable to the management of "physical" keys, and on March 8, 2018, a new [REDACTED] Procedure was implemented. The enterprise-wide procedure is managed by [REDACTED]. To ensure continued success with the management of "physical" keys, at the end of the 1st quarter of 2018, the AAMs performed a quarterly review of their Area Access Log activity for "physical" keys to validate that the implemented procedure is being followed correctly.

Additionally, even before the onsite audit, the Responsible Entity has the following types of defense-in-depth for physical security installed to protect its High and Medium Impact Cyber Assets, and minimize any risk associated with unauthorized access. [REDACTED]

The defense-in-depth discussion above is particularly pertinent to the security of the Medium Impact Substations where multiple layers of security would allow for the identification of any suspected activity in the vicinity of, or at the asset, which allows for notification to the Responsible Entity's Security and/or local law enforcement immediately upon detection. The risk to the reliability of the BES is greatly reduced due to the Responsible Entity's robust defense-in-depth approach to physical and electronic security.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

[REDACTED] the probability of a repeat exposure since the access authorizations of the domain administrator accounts was immediately remedied, and the identified "physical" key deficiencies were not only corrected, but a sustainable and repeatable process was established. Additionally, training on proper procedures will help ensure individuals are executing the process as defined. There are also now preventive and detective controls incorporated into the program.

Attachments ()

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am [REDACTED]
 - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
 - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
 - I have read and am familiar with the contents of this Mitigation Plan
 - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED], please contact the [REDACTED] department to determine your assigned SPOC at:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

This item was signed by [REDACTED] on 7/20/2018

This item was marked ready for signature by [REDACTED] on 7/20/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[REDACTED]

Name of Standard of mitigation violation(s):

[REDACTED]

Requirement	Tracking Number	NERC Violation ID
R4.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

[REDACTED]

No Milestones Defined

Summary of all actions described in Part D of the relevant mitigation plan:

All Completion Summaries and milestone evidence has been upload to the Secure Working folder.

Description of the information provided to [REDACTED] for their evaluation *

All Completion Summaries and milestone evidence has been upload to the Secure Working folder.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIA Secure Folder and E-MAIL

October 24, 2018

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED] (CIP-004-6 R4)

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-004-6 R4	June 19, 2018

After review for completion on **October 24, 2018**, [REDACTED] staff finds that [REDACTED]
has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this
mitigation plan.

If you have any questions, please feel free to contact [REDACTED]

[REDACTED]

[REDACTED]

Attachment 6

- 6a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-005-5 R1 submitted May 30, 2018
- 6b. The Entity's Certification of Mitigation Plan Completion for CIP-005-5 R1 submitted September 18, 2018
- 6c. The Region's Verification of Mitigation Plan Completion for CIP-005-5 R1 dated May 8, 2018

This item was signed by [REDACTED] on 5/30/2018

This item was marked ready for signature by [REDACTED] on 5/30/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-005-5 R1.	[REDACTED]	[REDACTED]	05/30/2018	Region reviewing Mitigation Plan	Formal	

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name:

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard:

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R1.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

[REDACTED] the Responsible Entity "permitted Internet Control Message Protocol (ICMP) inbound and outbound communication through an Electronic Access Point (EAP) to its High and Medium Impact BES Cyber Systems without maintaining documentation supporting the reason it granted the communication access. As a result, [Responsible Entity] was not in compliance with the CIP Reliability Standard CIP-005-5 Requirement R1. [REDACTED]

[Attachments \(\)](#)

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this Mitigation Plan:

[Attachments \(\)](#)

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan

has been completed, to correct the Alleged or Confirmed violations identified in Part C.1 of this form:

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

1: Perform an Extent of Condition to mitigate ICMP non-compliance deficiencies identified in the audit report for Medium Impact Bulk Electric System (BES) Cyber Systems (BCS) Electronic Access Points (EAPs). Using the Responsible Entity's 1st Quarter 2017 CIP-002 BES Cyber System list, review all EAPs for Medium Impact BES Cyber Systems and ensure that implicit and/or configurable settings for ICMP access are disabled to the maximum extent possible. EAPs for Medium Impact BES Cyber Systems that require ICMP to be enabled, document the business or operational reason(s) ICMP access was granted. Deliverable is evidence that ICMP access for all

non-
ns
stems
for

Ps will be reported to the Regional Entities. Completed by July 12, 2017.

3: Update the current EAP rule guidelines for Medium and High Impact BCSs. Enhance the current EAP rule guidelines for Medium and High Impact BCSs, as necessary, as a single enterprise wide document. Identify EAP rules from the guidelines that are considered "high risk", (for example, the Subject Matter Experts (SMEs) determined "high risk" is the use of the word "any" in the source, destination, or service; Interactive Remote Access without an Intermediate System; and, no deny by default). The guidelines identified as "high risk" will be used to perform an Extent of Condition of High Impact BCS EAP rules, of which the RC BCSs are a subset. Deliverables are an enhanced enterprise wide Firewall Policy Guideline with high risk guidelines identified, and a document describing the original and post changes to the guidelines. Completed by October 13, 2017.

4: Perform an Extent of Condition to develop a complete inventory list of existing documentation. The inventory of documentation will include policies, procedures, work instructions, drawings, implementation evidence templates (if applicable), and business justification for BCS EAP rules. The Business Units (BUs) are responsible for compliance and will create an inventory list of all existing documentation. BU Leaders and SMEs will be asked to provide all documentation and templates used to support compliance. A centralized location will be used to store the documentation or templates, and any links to documentation or templates. Inventory report will include the documentation or template name/number, BU owner, effective date, and termination date for any documentation that is related to temporary rules. Deliverable is an inventory list of all documentation. Completed by November 1, 2017.

5: Perform an Extent of Condition Analysis of all the High Impact BCS EAPs to identify "high risk", (for example, the Subject Matter Experts (SMEs) determined "high risk" is the use of the word "any" in the source, destination, or service; Interactive Remote Access without an Intermediate System; and, no deny by default), per the guidelines developed in milestone 3, and classify each into one of the following: (a) mitigate now by disabling or modifying the rule; (b) mitigate by other means; or (c) mitigate as part of milestone 15. Develop a plan that prioritizes the mitigation of High Impact BCS EAPs with rules that are classified as (a) or (b) above. Deliverables are (i) list of rules considered "high risk" per High Impact BCS EAPs; (ii) classification of each "high risk" rule; and, (iii) mitigating actions for each rule identified as "high risk", and (iv) a plan that prioritizes the mitigation of the "high risk" rules. Completed by November 15, 2017.

6: Perform an Extent of Condition to identify and document all inbound and outbound access permissions and denials; and, the associated business justification for all High and Medium Impact EAPs. (The inventory will be analyzed as part of Milestone 9 for extraneous rules.) The inventory will be stored in a centralized location. This milestone is specific to Part 1.2; all External Routable Connectivity must be through an identified Electronic Access Point (EAP). Deliverable is a complete inventory list of all High and Medium Impact BCS EAP inbound and outbound access permissions and denials. Completed by December 6, 2017.

7: Perform an Extent of Condition to determine whether all High and Medium Impact BCAs, (and their associated Protected Cyber Assets (PCAs)), reside within an Electronic Security Perimeter (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 BES Cyber System list, confirm that all applicable cyber assets reside within a defined ESP. Identify all EAPs on the ESP diagrams and check that all BCA and PCA connectivity is through an EAP. (Any asset(s) identified as BCA or PCA that does not reside within an identified ESP will be mitigated as part of Milestone 15.) This milestone is specific to Part 1.1, all applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP, and Part 1.2, all External Routable Connectivity must be through an identified EAP. Deliverable is evidence that all High and Medium Impact BCAs (and associated PCAs) reside within an ESP, and all external connectivity is through an EAP which will be proved by: (i) Network drawings of all ESP(s) and EAPs; (ii) Lists and/or drawings that demonstrate that all BCAs reside inside the ESP(s); (iii) Lists and/or drawings that demonstrate that all PCAs reside inside the ESP(s); (iv) Lists and/or drawings of all BES Cyber Systems inside the ESP(s) and their impact rating; and, (v) Network drawings and/or lists of all ESP Network topology identifying ESP(s) with and without External Routable Connectivity. Completed by January 31, 2018.

8: Working with the inventory report from the Extent of Condition in Milestone 4, IT will determine how the evidence should be structured, and how the implementation evidence template will be a repeatable, sustainable process. The enterprise-wide templates will be used to perform a consistent Extent of Condition across all BCS EAPs and will include (1) List of all ESPs with the applicable cyber assets that reside within the ESP, and which are connected via routable protocol; (2) Network Diagrams and/or lists depicting the ESP that consistently identifies: (a) All external routable communication paths, (b) All Electronic Access Points (EAPs), (c) Cyber Assets logically located within the ESP, (d) Cyber Assets allowing interactive remote access, and (e) Cyber Assets used for detecting malicious communication; (3) Documented firewall rule(s) that at a minimum include the business justification and technical guidelines for firewall rules developed in Milestone 3; (4) Dial-up connectivity (if needed for future); and (5) Methods used for detecting malicious communication and implementation steps. Policies, procedures, and work instructions will be addressed in Milestone 12. Completed by February 28, 2018.

9: Using the inventory list from the Extent of Condition in Milestone 6, and the guidance documentation and template(s) created in Milestone 8, determine 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, requiring inbound and outbound access permissions, (including those related to temporary rules), the reason for granting access, and deny all other access by default. Deliverable will be the discovery of any discrepancies for firewall rule(s) when compared to guidance documentation which will be reported to the Regional Entities and will be mitigated as part of Milestone 15. Completed by March 28, 2018.

10: Using the identified BCS EAP inventory list for all High and Medium Impact BCS at Control Centers, perform an Extent of Condition to verify that there is at least one method of detecting malicious communication for all inbound and outbound communications. This milestone is specific to Part 1.5, to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. Deliverable will be (i) a list of any EAPs that do not have at least one method of detecting malicious communication; and (ii) a documented list per ESP of the method(s) used to detect malicious communication. EAPs that do not have at least one method of detecting malicious communication will be reported to the Regional Entities and will be mitigated as part of Milestone 15. Completed by April 18, 2018.

11: Perform a Root Cause Analysis (RCA). The BUs will perform a RCA to identify the actual root cause(s). This milestone will address the following parts of Requirement R1: Part 1.1, all applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP; Part 1.2, all External Routable Connectivity must be through an identified Electronic Access Point (EAP); Part 1.3, require inbound and outbound access permissions, (including those related to temporary rules), the reason for granting access, and deny all other access by default; Part 1.4, certification that no Dial-up Connectivity is used for High and Medium Impact BCAs; and, Part 1.5, have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. Deliverable will be a Root Cause Analysis Report of the results. Completed by May 23, 2018.

12: Create 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 BUs will modify or develop controls for processes to make them repeatable and sustainable. This includes the development of an EAP Policy / Rule guideline that includes guidelines for temporary rules. The documents will 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 BES Cyber System list. Deliverable is the submission of processes and procedures that are repeatable and sustainable. The processes and procedures will include controls and steps to follow if a control fails for existing or new ESPs and/or devices. To be completed by June 15, 2018.

13: Develop training for new and updated documentation and implementation evidence templates, and provide training to Personnel. The BUs will: (1) Develop an enterprise-wide training program for CIP-005 R1 compliance documentation, to include updates when documentation is created or revised; (2) Determine who is required to take the training; (3) Define frequency and triggers for initiating training; (4) Define process to determine if training was effective; (5) Implement mechanism to document that training took place; and, (6) Conduct training. Deliverable is an enterprise-wide training program. To be completed by July 2, 2018.

14: Communicate to all SMEs and users, information about the new or updated policies, procedures and work instructions. All new or updated policies, procedures and work instructions will be revealed to the SMEs and users as they become effective. (NOTE: This milestone will document when all the new or updated policies, procedures and work instructions are effective. Some will become effective before this milestone completion date.) To be completed by August 1, 2018.

15: Correct any deficiency found in previous milestones. Utilizing all new or updated policies, procedures, work instructions, and training, correct all deficiencies identified in previous milestones. Additionally, any changes to, additions or deletions of BCS EAP assets from the Responsible Entity's 1st Quarter 2017 CIP-002 BES Cyber System lists used for this Mitigation Plan will be identified, and if necessary, mitigated per the new or updated policies, procedures, work instructions and training. To be completed by September 18, 2018.

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed. Attach the completed Mitigation Plan to this document. State whether the Mitigation Plan has been fully implemented:

9/18/2018

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

Create 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.

Milestone Pending (Due: 6/15/2018)

The Business Units will modify or develop controls for processes to make them repeatable and sustainable. This includes the development of an EAP Policy / Rule guideline that includes guidelines for temporary rules. The documents will 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 BES Cyber System list. Deliverable is the submission of processes and procedures that are repeatable and sustainable. The processes and procedures will include controls and steps to follow if a control fails for existing or new ESPs and/or devices.

Develop training for new and updated documentation and implementation evidence templates, and provide training to Personnel.

Milestone Pending (Due: 7/2/2018)

The Business Units will: (1) Develop an enterprise-wide training program for CIP-005 R1 compliance documentation, to include updates when documentation is created or revised; (2) Determine who is required to take the training; (3) Define frequency and triggers for initiating training; (4) Define process to determine if training was effective; (5) Implement mechanism to document that training took place; and, (6) Conduct training. Deliverable is an enterprise-wide training program.

Communicate to all SMEs and users, information about the new or updated policies, procedures and work instructions.

Milestone Pending (Due: 8/1/2018)

All new or updated policies, procedures and work instructions will be revealed to the SMEs and users as they become effective. (NOTE: This milestone will document when all the new or updated policies, procedures and work instructions are effective. Some will become effective before this milestone completion date.)

Correct any deficiency found in previous milestones.

Milestone Pending (Due: 9/18/2018)

Utilizing all new or updated policies, procedures, work instructions, and training, correct all deficiencies identified in previous milestones. Additionally, any changes to, additions or deletions of BCS EAP assets from the Responsible Entity's 1st Quarter 2017 CIP-002 BES Cyber System lists used for this Mitigation Plan will be identified, and if necessary, mitigated per the new or updated policies, procedures, work instructions and training.

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

The Responsible Entity has taken a comprehensive approach to this Mitigation Plan that will be completed on September 18, 2018, and is responsive to the possible violation (PV) in the Final Audit Report. With regard to abatement of interim risks attributable to the PV, for the following reasons, the Responsible Entity believes that there was, and continues to be, only minimal risk to the reliability of the Bulk Electric System (BES) during the execution and completion of this Mitigation Plan.

[REDACTED]

As a result of these additional firewalls and network protections, the risk of unauthorized access by an external party through ICMP at the Medium Impact BES Cyber System is very low.

At the completion of the onsite audit, the Responsible Entity promptly took steps to remediate the Internet Control Message Protocol (ICMP) issue for the specific Cyber Assets associated with the High and Medium Impact BES Cyber Systems cited in the Final Audit Report. ICMP is a supporting protocol used by network devices to send error messages and operational information. The Responsible Entity uses ICMP to monitor and access the availability and health of individual devices; and, to generate tickets for Network Operations when a device no longer operates properly, or is out of service. ICMP is an integral part of the Electronic Management System (EMS) and will ping other systems throughout the system's infrastructure to assess current status, check network responsiveness, and routing paths across the network, to list just a few.

By March 23, 2017, all ICMP firewalls were identified, and changes were implemented for the firewall access rules to complete [REDACTED] ES [REDACTED] ified during the onsite audit. By July 12, 2017, all ICMP firewalls were identified, and changes were implemented for the firewall access rules to complete remediation for all High Impact BES Cyber Systems. While conducting the Extent of Conditions for all High and Medium Impact BES Cyber System, the Responsible Entity confirmed that implicit and/or configurable settings for ICMP access were disabled completely, or to the maximum extent possible. For the High and Medium Impact BES Cyber Systems' EAPs that require ICMP to be enabled, the business or operational reason(s) or justification(s) for granting ICMP access for the EAP had a business justification that was documented.

[REDACTED]

The risk of unauthorized access by an external party through the ICMP was very low because the SME was able to access the EAP at the Medium Impact BES Cyber System only after logging into, with two-factor authentication, in order to get through multiple layers of firewalls and network protections, as described earlier.

[REDACTED]

On July 14, 2017, the Responsible Entity implemented its revised [REDACTED] The EAP guidelines and rules now include a detailed explanation of: (1) the "High-risk" rules, (i.e., use of "any" in the source, destination, or service; Interactive Remote Access without an Intermediate System; no deny by default); (2) the specific requirements from CIP-005-5 Requirement R1, Parts 1.1, 1.2, 1.3., 1.4 and 1.5; (3) the makes and models for all EAPs; and, (5) the enhanced controls based on security "best practices".

The firewall rules for each of the High and Medium Impact BES Cyber Asset EAPs will be fully remediated by September 28, 2018. Mitigation of the firewall rules at the

[Attachments \(\)](#)

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

At the completion of this Mitigation Plan, the Responsible Entity plans to have in place a comprehensive enterprise-wide program to effectively manage Electronic Access Points (EAPs) to High and Medium Impact BES Cyber Systems, including those with External Routable Connectivity, and access to Protected Cyber Assets (PCA). All ESPs for High and Medium Impact BES Cyber Systems will require inbound and outbound access permissions, with documented reasons for granting access, and deny by default for all other access. Authentication, where technically feasible will be required when establishing dial-up connectivity to Cyber Assets. Firewalls will be implemented to detect, isolate and record malicious communications.

Program documentation will include detailed guidelines and instructions for EAPs. Personnel will be adequately trained on updated policies, processes and templates. ESP drawings will be standardized, and lists of assets within the ESP will be continuously validated and updated, as necessary. There will be records showing clear business justifications for EAPs, with thorough checklists maintained.

[Attachments \(\)](#)

SECTION F: AUTHORIZATION

- An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:
- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
 - b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
 - c) Acknowledges:
 - I am [REDACTED]
 - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
 - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
 - I have read and am familiar with the contents of this Mitigation Plan
 - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED], please contact the [REDACTED] department to determine your assigned SPOC at:

[REDACTED]

[REDACTED]

[REDACTED]

This item was signed by [REDACTED] on 9/18/2018

This item was marked ready for signature by [REDACTED] on 9/18/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

Name of Standard of mitigation violation(s):

Requirement	Tracking Number	NERC Violation ID
R1.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

[Create 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.](#)

Milestone Completed (Due: 6/15/2018 and Completed 6/15/2018)

[Attachments \(0\)](#)

The Business Units will modify or develop controls for processes to make them repeatable and sustainable. This includes the development of an EAP Policy / Rule guideline that includes guidelines for temporary rules. The documents will 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 BES Cyber System list. Deliverable is the submission of processes and procedures that are repeatable and sustainable. The processes and procedures will include controls and steps to follow if a control fails for existing or new ESPs and/or devices.

[Develop training for new and updated documentation and implementation evidence templates, and provide training to Personnel.](#)

Milestone Completed (Due: 7/2/2018 and Completed 7/2/2018)

[Attachments \(0\)](#)

The Business Units will: (1) Develop an enterprise-wide training program for CIP-005 R1 compliance documentation, to include updates when documentation is created or revised; (2) Determine who is required to take the training; (3) Define frequency and triggers for initiating training; (4) Define process to determine if training was effective; (5) Implement mechanism to document that training took place; and, (6) Conduct training. Deliverable is an enterprise-wide training program.

[Communicate to all SMEs and users, information about the new or updated policies, procedures and work instructions.](#)

Milestone Completed (Due: 8/1/2018 and Completed 7/31/2018)

[Attachments \(0\)](#)

All new or updated policies, procedures and work instructions will be revealed to the SMEs and users as they become effective. (NOTE: This milestone will document when all the new or updated policies, procedures and work instructions are effective. Some will become effective before this milestone completion date.)

[Correct any deficiency found in previous milestones.](#)

Milestone Completed (Due: 9/18/2018 and Completed 9/18/2018)

[Attachments \(0\)](#)

Utilizing all new or updated policies, procedures, work instructions, and training, correct all deficiencies identified in previous milestones. Additionally, any changes to, additions or deletions of BCS EAP assets from the Responsible Entity's 1st Quarter 2017 CIP-002 BES Cyber System lists used for this Mitigation Plan will be identified, and if necessary, mitigated per the new or updated policies, procedures, work instructions and training.

Summary of all actions described in Part D of the relevant mitigation plan:

As of the completion of Milestone 15, all deficiencies have been addressed and the evidence will be uploaded to the Secure Working Folder as agreed to during conference call with enforcement on September 17, 2018.

Description of the information provided to FRCC for their evaluation *

As of the completion of Milestone 15, all deficiencies have been addressed and the evidence will be uploaded to the Secure Working Folder as agreed to during

conference call with enforcement on [REDACTED]

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

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIA Secure Folder and E-MAIL

May 8, 2019

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED] (CIP-005-5 R1)

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-005-5 R1	September 18, 2018

After review for completion on **May 7, 2019**, FRCC Compliance staff finds that [REDACTED] has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact [REDACTED]

[REDACTED]

[REDACTED]

Attachment 7

- 7a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-006-6 R1 submitted February 26, 2018
- 7b. The Entity's Certification of Mitigation Plan Completion for CIP-006-6 R1 submitted May 8, 2018
- 7c. The Region's Verification of Mitigation Plan Completion for CIP-006-6 R1 dated October 28, 2018

 A [previous version](#) of this Mitigation Plan exists

 This item was signed by [REDACTED] on 2/26/2018

 This item was marked ready for signature by [REDACTED] on 2/26/2018

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name:

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard:

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R1.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

[REDACTED] "did not implement two or more different physical access controls to allow unescorted physical access into its Local Backup Control Center (LBCC) Physical Security Perimeter (PSP) as required by the standard." [In footnote at 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."

"As a result, [Responsible Entity] was not in compliance with the CIP Reliability Standard CIP-006-6 Requirement R1. [REDACTED]"

"The LBCC is a control center with High Impact BES Cyber Systems identified by [Responsible Entity]. The LBCC PSP drawings identify an emergency exit door During the site visit of this location, the audit staff found that this emergency exit door allowed unescorted physical access into the LBCC PSP upon the press of a button without any authentication. The audit staff noted that this button allowed access into the PSP, not out of the PSP. Although such access activated a loud audible alarm, a single button granted the access into the PSP, which is contrary to the requirements." (p.14)

[Attachments \(\)](#)

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this Mitigation Plan:

The local back-up system control center assets are utilized by the Responsible Entity to perform functions for the reliable operation of the BES. The functional obligations were implicated by the possible violation remediated by this Mitigation Plan in the sense that the faulty PSP emergency exit door was part of the Responsible Entity's physical access control program for the local back-up control center that is intended to only be used during emergencies. Given the important security objective of controlling access to back-up system control centers, the Responsible Entity made every effort to complete this Mitigation Plan in a timely and thorough manner to minimize the likelihood of future similar non-compliance findings.

[Attachments \(\)](#)

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan

has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

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

- 1: Update the Physical Security Perimeter (PSP) at the Backup Control Center site to remove the foyer area. The Responsible Entity's Business Unit (BU) will remove the foyer door programming from the Physical Access Control System (PACS). Following this change, the BU will no longer monitor the foyer as a PSP. Completed by October 19, 2016.
- 2: Revise/update the Physical Security Perimeter drawing for the Backup Control Center to properly illustrate the foyer area and its authentication controls. Completed by December 7, 2016.
- 3: Review each High Impact PSP design by conducting a walkdown. Ensure no entry by key core, push button, etc., into the PSP from an egress only door. If access to a High Impact PSP by an egress only door is identified during the walkdown, it will be reported to the Regional Entity. Completed by March 24, 2017.
- 4: Correct any egress only doors that allow entry into a High Impact PSP found during walkdown in Milestone 3. For any identified egress only doors that allow entry into a High Impact PSP, correct the deficiency and/or remove entry mechanism. Completed by April 28, 2017.
- 5: Review Enterprise-wide Physical Security Plan to determine whether design expectations related to egress only doors are described within the Physical Security Plan. Completed by May 10, 2017.
- 6: Conduct training on the design expectations for egress only doors. Responsible Entity will schedule and administer a training session for physical security design Personnel on the design expectations required for egress only doors. Completed by May 10, 2017.
- 7: Revise [REDACTED] Procedure to include instructions that physical security drawings should be reviewed as part of a [REDACTED] walkdown, discuss with the Business Unit any changes or modifications that may have been made prior to the walkdown, and document exceptions identified during the walkdown. Completed by June 30, 2017.
- 8: Train [REDACTED] on the Updated [REDACTED] Procedure. This milestone involves: (1) Identifying the complete population of [REDACTED] (2) Preparing training materials, (i.e., presentation) and scheduling training session; and, (3) Delivering training to [REDACTED]. Completed by October 31, 2017.

Attachments ()

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

10/31/2017

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

No Milestones Defined

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

The Responsible Entity does not believe the reliability of the Bulk Power System (BPS) was at a higher risk, or negatively impacted, while this Mitigation Plan was being implemented. Although the emergency exit door into the PSP did not have authentication control upon entry, there were several additional security measures in place for this access door, (i.e., monitored access control alarming, local audible alarm, two-factor readers inside the foyer space), that reduced the likelihood of misuse or undetected unauthorized access to High Impact BES Cyber Systems.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

This Mitigation Plan was drafted to ensure it would minimize the likelihood of further violations of the physical access control requirements for PSPs housing High Impact BES Cyber Systems. The access door no longer allows the possibility of entry into the PSP, therefore the probability of reoccurrence for the specific location highlighted in the final audit report has been eliminated. Likewise, all other PSPs housing High Impact BES Cyber Systems have been inspected to ensure no egress door can be used as an ingress point, which will help mitigate the risk of future similar violations at other locations. Additionally, the Procedure for PSP reviews where High Impact BES Cyber Systems are housed has been revised to strengthen the review and oversight process for managing Physical Security Perimeters, and all [REDACTED] Managers have been trained.

Attachments ()

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am [REDACTED]
 - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
 - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
 - I have read and am familiar with the contents of this Mitigation Plan
 - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED], please contact the [REDACTED] litigation department to determine your assigned SPOC at:

[REDACTED]

[REDACTED]

[REDACTED]

This item was signed by [REDACTED] on 5/18/2018

This item was marked ready for signature by [REDACTED] on 5/18/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[REDACTED]

Name of Standard of mitigation violation(s):

[REDACTED]

Requirement	Tracking Number	NERC Violation ID
R1.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

[REDACTED]

No Milestones Defined

Summary of all actions described in Part D of the relevant mitigation plan:

The Milestone Completion Summaries have been uploaded to the Secure Working folder.

Description of the information provided to FRCC for their evaluation *

The Milestone Completion Summaries have been uploaded to the Secure Working folder.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIA Secure Folder and E-MAIL

October 24, 2018

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED] (CIP-006-6 R1)

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-006-6 R1	February 26, 2018

After review for completion on **October 24, 2018**, [REDACTED] staff finds that [REDACTED]
has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this
mitigation plan.

If you have any questions, please feel free to contact [REDACTED]

[REDACTED]

[REDACTED]

Attachment 8

- 8a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-006-3c R1 submitted May 24, 2018
- 8b. The Entity's Certification of Mitigation Plan Completion for CIP-006-3c R1 submitted June 11, 2018
- 8c. The Region's Verification of Mitigation Plan Completion for CIP-006-3c R1 dated October 24, 2018

This item was signed by [REDACTED] on 5/23/2018

This item was marked ready for signature by [REDACTED] on 5/23/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation IDs	Date Submitted	Status	Type	Revision Number
CIP-006-6 R2.	[REDACTED]	[REDACTED]	05/23/2018	Region reviewing Mitigation Plan	Formal	

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name:

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard:

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R2.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

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

"[Responsible Entity] maintained visitor access logs that documented access into its PSPs. The audit team reviewed the access logs at [Responsible Entity's Datacenter] PSP and found that on several occasions visitors signed into the PSP, entering data for the time-in field, but the time-out fields for these visitors were not populated in the logs. CIP-006-6 R2.2 requires that [Responsible Entity] log visitors' entries into and exits out of the PSP. Moreover, the log must be populated with the date and time of the initial entry and last exit. [Responsible Entity's] visitor access logs were deficient and not consistent with this Reliability Standard requirement." (p.15)

Attachments ()

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this Mitigation Plan:

[REDACTED] want to note that the Physical Security Perimeters (PSPs) at the Datacenter identified in the Final Audit Report do not include or encompass the entire floor, but instead are made up of four (4) distinct file cabinets. [REDACTED] stated that these visitors were on the floor but not necessarily entering the PSPs. In any event, the functional obligations of the Responsible Entity's System Control Center were indirectly implicated by the PV remediated by this Mitigation Plan. The deficient visitor logs that form the basis of the PV were located at a data center that hosts Electronic Access Control and Monitoring Systems (EACMS) management servers that are used to control access to High Impact Bulk Electric System (BES) Cyber Systems. Given the important security objective of accurately tracking visitor access to EACMS within the data centers, the Responsible Entity completed this Mitigation Plan in a timely and thorough manner to minimize the likelihood of future similar non-compliance findings.

Attachments ()

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it has undertaken, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

- 0: The Responsible Entity's preliminary assessment identified two reasons for the possible violation finding. First, the Responsible Entity's process for quarterly review of visitor access logs was inadequate. Second, individuals with authorized unescorted physical access to PSPs were not trained well enough to understand and meet the required level of responsibility when signing visitors in and out of PSPs, and ensuring the recording of all date and time information for each person. Completed by December 31, 2016.
- 1: Evaluate the process for reviewing visitor access logs and identify enhancements that need to be incorporated, including creating new controls and strengthening existing controls. Completed by February 20, 2017.
- 2: Review process for signing visitors in and out of PSPs. Review the process that is utilized by those who have authorized unescorted physical access; and, identify enhancements that need to be incorporated including creating new controls and strengthening existing controls. Completed by February 28, 2017.
- 3: Perform an Extent of Condition analysis by reviewing visitor log entries to all PSPs of the Responsible Entity during the time period starting March 2015 to 4 h quarter of 2016. Completed by April 28, 2017.
- 4: Modify visitor log process for signing visitors in-and-out of PSPs, and incorporate enhancements identified in Milestones 1 and 2 into the modified process. Completed by September 8, 2017.
- 5: Review the PSP visitor logs and identify all instances where the escort can correct deficient log entries missing required data, and close out the missing log entries. Completed by November 17, 2017.
- 6: Schedule and administer training with the employees and independent contractors who are responsible for monitoring, managing and reviewing visitor logs according to the revised processes. Completed by December 15, 2017.

Attachments ()

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

12/15/2017

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

No Milestones Defined

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

The Responsible Entity developed a Mitigation Plan in response to this PV that was completed on December 15, 2017. For the following reasons the Responsible Entity believes there was minimal risk to the reliability of the Bulk Electric System (BES) both before and after the Responsible Entity developed and executed this Mitigation Plan.

[REDACTED] As a result, there was virtually no risk that someone on the floor without authorization could access the CIP assets in this manner.

Further, any potential risk associated with this administrative issue, (i.e., entering the visitor's "time out" in the log book), was largely mitigated by compliance with the Responsible Entity's procedures requiring the escort to remain with the visitor at all times, assuring that the visitor only had access to the areas, materials, and systems in which he or she was working. This policy and process significantly mitigated any potential risk associated with the fact that the specific time of departure from the PSP or the floor was not recorded on the log.

The strongest protection of the integrity and security of the Responsible Entity's Cyber Assets while visitors are being provided access is the vigilance of the escort responsible for that visitor. While the time a visitor has signed out of a PSP should be included in the visitor log in accordance with CIP requirements and the Responsible Entity's policies, the risk of unauthorized access to the Responsible Entity's Cyber Assets is best protected and largely mitigated through the eyes and ears of its escorts. For the foregoing reasons, the Responsible Entity believes there was minimal risk to the BES due to the log deficiencies identified in the Final Audit Report, all of which have been remedied through successful completion of the Mitigation Plan and the subsequent actions of the Responsible Entity.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

Successfully completing this Mitigation Plan ensures that the Responsible Entity has accurate records of those visitors who are granted escorted access to a PSP. Completion of this Mitigation Plan will also ensure that the Subject Matter Experts (SMEs) responsible for performing the reviews on a quarterly basis are equipped with the appropriate training to perform the task, and that those who have authorized unescorted physical access receive the proper training to ensure their visitors are signed in and out of the PSPs. Execution of these improvements will minimize the likelihood of further violations of the visitor control program.

Attachments ()

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and

- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and

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

- c) Acknowledges:

- I am [REDACTED]
- I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
- I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
- I have read and am familiar with the contents of this Mitigation Plan
- [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED] please contact the [REDACTED] department to determine your assigned SPOC at:

[REDACTED]

[REDACTED]

[REDACTED]

This item was signed by [REDACTED] on 6/11/2018

This item was marked ready for signature by [REDACTED] on 6/11/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[REDACTED]

Name of Standard of mitigation violation(s):

[REDACTED]

Requirement	Tracking Number	NERC Violation ID
R2.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

[REDACTED]

No Milestones Defined

Summary of all actions described in Part D of the relevant mitigation plan:

Completion Summaries and all supporting evidence were uploaded to the Secure Working folder.

Description of the information provided to FRCC for their evaluation *

Completion Summaries and all supporting evidence were uploaded to the Secure Working folder.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIA Secure Folder and E-MAIL

October 24, 2018

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED] (CIP-006-6 R2)

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-006-6 R2	May 23, 2018

After review for completion on **October 24, 2018**, [REDACTED] staff finds that [REDACTED]
has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this
mitigation plan.

If you have any questions, please feel free to contact [REDACTED].

[REDACTED]

[REDACTED]

Attachment 9

- 9a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-3a R2 submitted May 24, 2018
- 9b. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R2 submitted August 17, 2018
- 9c. The Region's Verification of Mitigation Plan Completion for CIP-007-3a R2 dated May 7, 2019

This item was signed by [REDACTED] on 5/24/2018

This item was marked ready for signature by [REDACTED] on 5/24/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-007-6 R1.	[REDACTED]	[REDACTED]	05/24/2018	Region reviewing Mitigation Plan	Formal	

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name: [REDACTED]

Company Address: [REDACTED]

Compliance Registry ID: [REDACTED]

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name: [REDACTED]

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard: [REDACTED]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R1.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

[REDACTED] alleges a possible violation of CIP-007-6 Requirement R1 based on findings that the Responsible Entity "did not properly document its need to have logical network accessible ports enabled for certain of its Bulk Electric System (BES) Cyber Assets"; and "did not properly document that certain of its BES Cyber Assets did not have a provision for disabling or restricting logical ports" (p.15). The BES Cyber Asset that formed the basis of the latter finding is used by the Responsible Entity in performance of the Reliability Coordinator (RC) function.

"Additionally, audit staff observed a demonstration of the authentication and login process for one of the [Responsible Entity's] GPS clock cyber assets during the site visit. The audit team discovered that the interface was coded in hypertext markup language (HTML) and it did not support the more secure hypertext transfer protocol secure (HTTPS) for network communication; log password changes or logins; support alerts for unsuccessful login attempts; or provide a lock-out feature. In addition, [a cyber] device used a shared administrator account password that was only required to be changed annually during [Responsible Entity's] annual performance of its Cyber Vulnerability Assessment. A [Responsible Entity] SME also informed the audit team that there are ports and services on the device that are not capable to be disabled. Although the cyber asset may not be able to meet the disable or restrict requirements of CIP-007-6, [Responsible Entity] is required to provide evidence that device has no provision for disabling or restricting logical ports", (p.16).

The Responsible Entity had not implemented viable processes and controls for documenting and enabling only logical network accessible ports and services that are deemed necessary. In addition, while the Responsible Entity's compliance group issued written guidance on Technical Feasibility Exceptions ("TFE") under Version 5 of the CIP Reliability Standards, the Responsible Entity lacked a documented process for determining if a TFE is necessary under Part1.1 of CIP-007-6 for devices that have no provision for disabling or restricting logical ports.

Attachments ()

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this MitigationPlan:

Representatives from multiple operational Business Units (BUs) [REDACTED] are working collaboratively on the milestone activities in this Mitigation Plan. Personnel from [REDACTED] are working together to develop enterprise-wide program documentation and controls; and, separately, on compliance responsibilities that are managed more effectively with processes, procedures and work templates designed specifically for their BU. The objective of this multi-departmental effort is to create an enterprise-wide program for the Responsible

The BUs will create enterprise-wide documented processes, work instructions, templates, and controls; develop training programs for all new enterprise-wide documentation; and, will retain all associated implementation evidence throughout execution of the plan. Evidence will be developed, documented, and consolidated, evaluating its use throughout the organization, and consolidating where appropriate; and, then finalizing the new enterprise-wide documentation, training, and subsequently implementing a comprehensive enterprise-wide program is expected to take a little less than one (1) year to complete.

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

[Attachments \(\)](#)

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

- 1: Create an inventory list of policies, standards, procedures, and work instruction documentation for ports and services currently in effect for [REDACTED] Business Units. Inventory list will include document name/number, Business Unit (BU) Owner, and effective date. Completed by September 8, 2017.
- 2: Develop an inventory list of all existing ports and services implementation evidence templates not previously identified in milestone 1 [REDACTED]. The output will be an inventory list of the evidence templates by name/number, BU Owner, and effective date. Completed by September 8, 2017.
- 3: Determine the sustainability of existing ports and services [REDACTED] in the inventory list created in milestone 2 [REDACTED]. Decide 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. The BUs will document what contents and instructions are usable to create enterprise-wide ports and services implementation evidence templates. Completed by September 8, 2017.
- 4: Evaluate the inventory list created in milestone 1 of effective policies, standards, procedures, and work instruction documentation for ports and services [REDACTED] to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable. The BUs will document what content, instructions, and tools in the policies, standards, procedures, and work instruction documentation for ports and services currently in effect [REDACTED] is usable and can be combined into corporate-wide documentation. Completed by September 15, 2017.
- 5: Perform an Extent of Condition (EOC). Working with the 1st Quarter 2017 CIP-002 BES Cyber System list, the BUs will determine if all enabled ports and services are documented for all applicable devices. The output will be a complete, comprehensive inventory of applicable devices with enabled ports and services, output from the devices to substantiate enabled ports and services, the business justification, and evidence from the vendor. Additional findings of undocumented enabled ports and services will be reported to the Regional Entities. Completed by October 23, 2017.
[REDACTED]
[REDACTED]
[REDACTED] analysis. Possible Root Cause(s) will be identified. Any additional findings of non-compliance will be reported to the Regional Entities. Completed by October 25, 2017.
[REDACTED]
[REDACTED] contributing factors. Completed by October 27, 2017.
- 8: Develop a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the Root Cause Analysis in milestone 7. Completed by November 24, 2017.
- 9: Develop enterprise-wide documentation for ports and services. The enterprise-wide documentation will be supplemented with processes that specifically address: (A) Determination of devices for enabled ports and services.; (B) Documenting the need for enabled ports and services. (For ephemeral ports, evaluate and document the need for port ranges. This can come from vendor documentation and BU SME input according to how or where the device is used, and output from milestone 6. This determination will be an enterprise-wide methodology.); (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) Documenting the process on how the BUs determine if a TFE is necessary for Part 1.1. This will include a device type where the device has no provision for disabling ports and/or services, and there is no vendor documentation to support disabling. A TFE will be created.; and, (E) The process on how to protect against the use of unnecessary physical input/output ports. The process will include what the execution evidence would look like, (e.g. annual CVA check for port locks, system configuration for logically disabled ports, etc.). Completed by December 22, 2017.
- 10: Determine Roles and Responsibilities. Identify ownership of devices by BU to ensure coverage for all ports and services. The BUs will collaboratively determine and document who is responsible for specific inventoried devices based on location. The BUs will document the responsible BU and the SMEs, Groups, and/or Departments who are responsible for the ports and services for those devices. This mitigating action will also include identifying who is responsible for administering training. Completed by December 22, 2017.
- 11: The CIP Senior Manager and BU Directors will review the results of Milestone 10 and agree to the designated BU ownership of devices, and their obligation to maintain processes, evidence and training for ports and services. A letter will be drafted and signed by the CIP Senior Manager and BU Directors agreeing to assigned ports and services responsibilities for specific inventoried devices, including training. Completed by January 25, 2017.
- 12: The BUs will develop controls for ports and services documentation so that they are repeatable and sustainable. Controls for creating and maintaining all ports and service documentation, and implementation evidence templates, will be included in the Roles and Responsibilities' agreements developed in Milestone 11. Completed by January 26, 2017.
- 13: Develop implementation evidence templates for ports and services. The BUs will create enterprise-wide implementation evidence templates for capturing evidence for ports and services. The templates will have common nomenclature to be used enterprise-wide and will include: (a) device name; (b) enabled and listening ports; (c) port ranges if applicable; (d) services; (e) business justification; (f) columns to capture what is being measured; (g) revision history; and, (h) proper "Confidential – CEII" headers or footers. Completed by February 16, 2018.
- 14: Develop Training program for new and updated ports and services documentation and implementation evidence templates. The BUs will develop an enterprise-wide Training program for when ports and services documentation and/or implementation evidence templates are created or updated. Personnel listed in the 'Roles and Responsibilities' section of the ports and services documentation and implementation evidence templates, and anyone identified as needing the training, will be required to complete the training. Also, each BU will designate who is responsible for administering, maintaining, updating and tracking completion of the training program for ports and services. Completed by April 6, 2018.
- 15: Perform Training. The BUs will determine 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. Completed by May 18, 2018.
- 16: Implement countermeasures, updated documentation, templates, and controls. The BUs will implement the updated ports and services documentation, templates, and controls that will cover: (A) Part 1.1: a completed ports and services implementation evidence template that includes device names, enabled ports and port ranges if applicable, services, business justification, and completed revision history for all devices in the High and Medium Impact BES Cyber Systems list; and, (B) Part 1.2: evidence that physical ports are protected on all High Impact BCS and their associated EACMS, PACS, and PCA. Evidence will include documentation, screenshots of unneeded physical ports being disabled, signage or tamper tape that is attached to the devices, or screenshots of port locks on applicable devices. To be completed by August 17, 2018.

[Attachments \(\)](#)

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

8/17/2018

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

The BUs will implement the updated ports and services documentation, templates, and controls that will cover: (A) Part 1.1: a completed ports and services implementation evidence template that includes device names, enabled ports and port ranges if applicable, services, business justification, and completed revision history for all devices in the High and Medium Impact BES Cyber Systems list; and, (B) Part 1.2: evidence that physical ports are protected on all High Impact BCS and their associated EACMS, PACS, and PCA. Evidence will include documentation, screenshots of unneeded physical ports being disabled, signage or tamper tape that is attached to the devices, or screenshots of port locks on applicable devices.

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

With regard to remote electronic access and putative risks posed by the PV for CIP-007-6 Requirement R1, the following narrative describes the steps that an external unauthorized user, (i.e., a user that has not been granted electronic CIP access authorization in accordance with CIP-004-6), would have to take in order to gain remote electronic access to ports and services of the type for High and Medium BES Cyber Assets referenced in the Final Audit Report.

Meanwhile, comparable levels of protection for Medium Impact BES Cyber Systems associated with Generation facilities are overseen by plant specific cyber security managers. [REDACTED]

In summary, while the Mitigation Plan is not scheduled to be completed until August 17, 2018, the risk to the reliability of the BES is greatly reduced due to the Responsible Entity's robust defense-in-depth approach to physical and network security.

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

By successfully completing this Mitigation Plan, the Responsible Entity will reduce the risk of future violations and ensure sustainable compliance. At the completion of the

Mitigation Plan, the Responsible Entity will have:

- o Enterprise-wide documentation capturing sustainable, repeatable processes and controls for documenting enabled logical network accessible ports and services, including the business justification;
- o A training program that ensures all Personnel with documented 'Roles and Responsibilities' will be trained on the new and/or updated processes; and,
- o Enterprise-wide implementation evidence templates to capture enabled logical network accessible ports, services, and business justification.

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

[Attachments \(\)](#)

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am [REDACTED]
 - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
 - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
 - I have read and am familiar with the contents of this Mitigation Plan
 - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED] please contact the [REDACTED] department to determine your assigned SPOC at:

[REDACTED]

[REDACTED]

[REDACTED]

This item was signed by [REDACTED] on 8/17/2018

This item was marked ready for signature by [REDACTED] on 8/17/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

Name of Standard of mitigation violation(s):

Requirement	Tracking Number	NERC Violation ID
R1.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

[Implement countermeasures, updated documentation, templates, and controls.](#)

Milestone Completed (Due: 8/17/2018 and Completed 8/17/2018)

[Attachments \(0\)](#)

The BUs will implement the updated ports and services documentation, templates, and controls that will cover: (A) Part 1.1: a completed ports and services implementation evidence template that includes device names, enabled ports and port ranges if applicable, services, business justification, and completed revision history for all devices in the High and Medium Impact BES Cyber Systems list; and, (B) Part 1.2: evidence that physical ports are protected on all High Impact BCS and their associated EACMS, PACS, and PCA. Evidence will include documentation, screenshots of unneeded physical ports being disabled, signage or tamper tape that is attached to the devices, or screenshots of port locks on applicable devices.

Summary of all actions described in Part D of the relevant mitigation plan:

Completion Summary and supporting evidence will be uploaded to the Secure Working folder.

Description of the information provided to [REDACTED] for their evaluation *

Completion Summary and supporting evidence will be uploaded to the Secure Working folder.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIA Secure Folder and E-MAIL

May 8, 2019

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED] (CIP-007-6 R1)

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-007-6 R1	August 17, 2018

After review for completion on May 7, 2019, [REDACTED] staff finds that [REDACTED] has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact [REDACTED]

[REDACTED]

[REDACTED]

Attachment 10

- 10a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-3a R3 submitted June 19, 2018
- 10b. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R3 submitted September 28, 2018
- 10c. The Region's Verification of Mitigation Plan Completion for CIP-007-3a R3 dated May 7, 2019

 This item was signed by [REDACTED] on 6/7/2018



 This item was marked ready for signature by [REDACTED] on 6/7/2018



MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-007-6 R2.	[REDACTED]	[REDACTED]	06/07/2018	Region reviewing Mitigation Plan	Formal	

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name: [REDACTED]

Company Address: [REDACTED]

Compliance Registry ID: [REDACTED]

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name: [REDACTED]

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard: [REDACTED]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R2.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

[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, [Responsible Entity's] process neither appropriately assessed the applicability of new security patches for Cyber Assets nor provided for the retention of tracking records that support the performance of tests of patches. [REDACTED]"

[Attachments \(\)](#)

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this Mitigation Plan:

Representatives from multiple operational Business Units (BUs), [REDACTED] are working collaboratively on the milestone activities in this Mitigation Plan. Personnel from [REDACTED] are working together to develop enterprise-wide program documentation and controls; and, separately, on compliance responsibilities that are managed more effectively with processes, procedures and work templates designed specifically for their BU. The objective of this multi-departmental effort is to create an enterprise-wide program for the Responsible Entity that is consistent across all BUs.

The BUs will create enterprise-wide documented processes, work instructions, templates, and controls; develop training programs for all new enterprise-wide documentation; and, will retain all associated implementation evidence throughout execution of the milestone activities. The effort involved in combining existing BU documentation, evaluating its use throughout the organization, and consolidating where appropriate; and, then finalizing the new enterprise-wide documentation, training, and subsequently implementing a comprehensive enterprise-wide program is expected to take a little less than one (1) year to complete.

[Attachments \(\)](#)

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing, or has completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

- 1: Create an inventory list of policies, standards, procedures, and work instruction documentation for security patch management currently in effect for [REDACTED] Business Units. Inventory list will include document name/number, Business Unit (BU) Owner, and effective date. Completed by September 8, 2017.
- 2: Develop an inventory list of all existing security patch management implementation evidence templates not previously identified in milestone 1 [REDACTED] BUs. The output will be an inventory list of the evidence templates by name/number, BU Owner, and effective date. Completed by September 8, 2017.
- 3: Determine the sustainability of existing security patch management implementation evidence templates in the inventory list created in milestone 2 [REDACTED] BUs. Decide 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. The BUs will document what contents and instructions are usable to create enterprise-wide security patch management implementation evidence templates. Completed by September 8, 2017.
- 4: Evaluate the inventory list created in milestone 1 of effective policies, standards, procedures, and work instruction documentation for security patch management [REDACTED] BUs to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable. The BUs will document what content, instructions, and tools in the policies, standards, procedures, and work instruction documentation for security patch management currently in effect [REDACTED] is usable and can be combined into corporate-wide documentation. Completed by September 15, 2017.
- 5: Perform an Extent of Condition (EOC). Working with the 1st Quarter 2017 CIP-002 BES Cyber System list, the BUs will identify if there is documentation for the hardware and/or software patching requirements which involve monitoring of vendors for possible patches. The output will be a comprehensive inventory of devices with the hardware and/or software patching requirements for all applicable devices which involve monitoring of vendors. Completed by October 23, 2017.
- 6: Perform an Extent of Condition (EOC) analysis to identify possible Root Cause(s). The BUs will perform an EOC analysis using the inventory of documentation and devices that were identified during execution of Milestones 1, 2, and 5. The compliance group will compile questions and perform BU SME interviews for additional input for the EOC analysis. The results of the interviews will be given to the BUs to incorporate into the EOC analysis. Possible Root Cause(s) will be identified as a result of the EOC Analysis. Any additional findings of non-compliance will be reported to the Regional Entities. Completed by October 25, 2017.
- 7: Perform a Root Cause Analysis to determine Root Cause(s) and contributing factor(s). The BUs will perform a Root Cause analysis and identify the root cause(s) and contributing factors. Completed by October 27, 2017.
- 8: Develop a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the Root Cause Analysis. Completed by December 22, 2017.
- 9: Determine Roles and Responsibilities. Identify ownership of devices by BU to ensure coverage. The BUs will collaboratively determine and document who is responsible for inventoried devices based on location. The BUs will document the responsible BU and the SMEs, Groups, and/or Departments who are responsible for compliance activities for those devices. This exercise will also determine who is responsible for administering training. Completed by December 22, 2017.
- 10: The CIP Senior Manager and BU Directors will review the results of Milestone 5 and agree to their designated BU ownership of devices, and their obligation to maintain processes, evidence and training. A letter will be drafted and signed by the CIP Senior Manager and BU Directors agreeing to assigned compliance responsibilities for specific devices, including training. Completed by January 25, 2018.
- 11: The BUs will create enterprise-wide documentation, which will include input from Milestone 4. The new enterprise-wide documentation will be supplemented with processes to ensure compliance. This will include: (A) A process for documenting contact with vendors every 35 calendar days on the availability of applicable security patches; (B) A process for the evaluation of security patches to include who performs the evaluation and the criteria used for determination; (C) A process for creating and revising mitigation plans for security patches that cannot be applied within 35 calendar days after the patch evaluation. The process will include actions to mitigate the vulnerabilities by each patch, timeframe for completing the mitigation plan, if an extension, the reason. For extensions, the process for notifying CIP Senior Manager for approval of the extension; (D) A process on applying security patches within 35 calendar days of evaluation. The process will include: (i) The responsible group for applying the patches; (ii) How the patches are applied: by device type, by location, are they manually applied, pushed by an intermediate system or by the vendor; and (iii) How and who documents when the patches are applied; and (E) If there are network scans provided as evidence, where they are stored, and who does the scans. Completed by January 31, 2018.
- 12: The BUs will develop controls for the CIP-007 processes to make them repeatable and sustainable. Controls for creating and maintaining all processes will be documented for the enterprise-wide documentation developed during the execution of Milestone 11. Completed by February 23, 2018.
- 13: The BUs will create enterprise-wide implementation evidence templates. The templates will have common nomenclature that will be used enterprise-wide. The templates will include: (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. How the evaluation was performed, who performed the evaluation, and the date of the evaluation; (C) Capturing the documentation that security patches were applied within 35 calendar days of evaluation; (D) Capturing the details of the mitigation plan to include: (i) How the vulnerability will be addressed while the patch is not applied; (ii) Timeframe for completion; (iii) Responsible BU/SME; (iv) Device type / name; (v) Vendor and patch number; and, (vi) If a revision, a place for CIP Senior Manager sign-off. Templates will also include revision history, proper "Confidential – CEII" headers or footers, columns or fields to capture the measures of the requirement. Completed by March 23, 2018.
- 14: Develop Training program for new and updated documentation and implementation evidence templates. The BUs will develop an enterprise-wide Training program for when documentation and/or implementation evidence templates are created or updated. Personnel listed in the 'Roles and Responsibilities' section of the documentation and implementation evidence templates, and anyone identified as needing the training, will be required to complete the training. Also, each BU will designate who is responsible for administering, maintaining, updating and tracking completion of the training program. Completed by May 11, 2018.
- 15: Perform Training. The BUs will determine 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. To be completed by June 29, 2018.
- 16: Implement new and/or updated CIP-007 documentation and controls. BUs will implement the new and /or updated documentation and controls, and submit implementation evidence for each Part of the CIP-007 Requirement R2: (A) Documentation of contact with vendors for applicable security patches every 35 calendar days; (B) Evaluation results of security patches, showing completion dates within 35 calendar days of being notified of a security patch release. Document how the evaluation was performed, by whom, and date of evaluation.; (C) Documentation that security patches were applied within 35 calendar days of evaluation. This will include how the patch was applied (manually, pushed by an intermediate device, pushed by the vendor), date of patch application and verification that the patch was successfully applied.; and, (D) Documentation of Mitigation Plan or revision to Mitigation Plan, planned actions to mitigate any vulnerabilities, timeframe for completion and approval of the Mitigation Plan by the CIP Senior Manager. To be completed by September 28, 2018.

Attachments ()

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

9/28/2018

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

Perform Training

Milestone Pending (Due: 6/29/2018)

The BUs will determine 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.

Implement new and/or updated CIP-007 documentation and controls.

Milestone Pending (Due: 9/28/2018)

BU's will implement the new and /or updated documentation and controls, and submit implementation evidence for each Part of the CIP-007 Requirement R2. (A) Documentation of contact with vendors for applicable security patches every 35 calendar days; (B) Justification results of security patching, showing completion dates within 35 calendar days of being notified of a security patch release. Document how the evaluation was performed, by whom, and date of evaluation.; (C) Documentation that security patches were applied within 35 calendar days of evaluation. This will include how the patch was applied (manually, pushed by an intermediate device, pushed by the vendor), date of patch application and verification that the patch was successfully applied.; and, (D) Documentation of Mitigation Plan or revision to Mitigation Plan, planned actions to mitigate any vulnerabilities, timeframe for completion and approval of the Mitigation Plan by the CIP Senior Manager.

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

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

Despite the security patching deficiencies highlighted in the final audit report, the risk to the reliability of the BES is minimal during the execution phase of this Mitigation Plan as the Responsible Entity's BES Cyber Systems will continue to be protected by strong physical and electronic security defense-in-depth controls that have been implemented for CIP-006-6 Requirements R1 and R2, and CIP-005-5 Requirement R2.

Four levels of protection and steps are required in order to remotely access all of the Electronic Access Points (EAPs) at the Responsible Entity's High and Medium Impact BES Cyber Systems. Further, all communications and access to EAPs at the Responsible Entity's Control Center High and Medium Impact BES Cyber Systems are permitted only through an encrypted network.

Meanwhile, comparable levels of protection for Medium Impact BES Cyber Systems associated with Generation facilities are overseen by plant specific cyber security managers.

Collectively, these protections greatly reduce any putative risk to the reliability of the BES that may be posed by the PV finding. Nevertheless, the Responsible Entity's Business Units (BUs) are aware of the security risk posed by inadequate security patching for devices and applications associated with its BES Cyber Systems. The training for the new enterprise-wide security patching procedure will be completed by June 15, 2018. Then the enterprise-wide security patching procedure and associated evidence templates will be implemented to immediately commence remediation for any Extent of Condition (EOC) issues. The enterprise-wide implementation for the security patching procedure and associated evidence templates is expected to be completed by September 28, 2018 based on the number of devices in scope. Since there are over [REDACTED] devices, at this time, it is not known if the three (3) month implementation time-period can be shortened and still allow for full remediation of the EOC issues, but every effort will be made to complete the implementation for the security patching procedure and associated evidence templates as soon as possible.

By completing all milestones in this Mitigation Plan, the Responsible Entity expects to greatly minimize any risk the PV finding may be deemed to pose to the BES and ensure that a sustainable program is in place to cover all Parts of Requirement R2. In the meantime, as noted above, the risk to the reliability of the BES is greatly reduced due to the Responsible Entity's robust defense-in-depth approach to physical and network security.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

By successfully completing this Mitigation Plan, the Responsible Entity will have in place:

- Enterprise-wide documentation consisting of sustainable, repeatable processes and controls for tracking, evaluating, installing and documenting cyber security patch updates;
- A formal training program to ensure all Personnel with documented Roles and Responsibilities are adequately, and periodically trained on the new and/or revised processes for security patch management; and,
- Enterprise-wide implementation evidence templates to completely capture the patch management process.

Attachments ()

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am [REDACTED]
 - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
 - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
 - I have read and am familiar with the contents of this Mitigation Plan
 - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED] please contact the [REDACTED] department to determine your assigned SPOC at:

[REDACTED]

This item was signed by [REDACTED] on 9/28/2018

This item was marked ready for signature by [REDACTED] on 9/28/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

Name of Standard of mitigation violation(s):

Requirement	Tracking Number	NERC Violation ID
R2.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

Perform Training

Milestone Completed (Due: 6/29/2018 and Completed 6/29/2018)

[Attachments \(0\)](#)

The BUs will determine 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.

Implement new and/or updated CIP-007 documentation and controls.

Milestone Completed (Due: 9/28/2018 and Completed 9/28/2018)

[Attachments \(0\)](#)

BUs will implement the new and /or updated documentation and controls, and submit implementation evidence for each Part of the CIP-007 Requirement R2: (A) Documentation of contact with vendors for applicable security patches every 35 calendar days; (B) Evaluation results of security patches, showing completion dates within 35 calendar days of being notified of a security patch release. Document how the evaluation was performed, by whom, and date of evaluation.; (C) Documentation that security patches were applied within 35 calendar days of evaluation. This will include how the patch was applied (manually, pushed by an intermediate device, pushed by the vendor), date of patch application and verification that the patch was successfully applied.; and, (D) Documentation of Mitigation Plan or revision to Mitigation Plan, planned actions to mitigate any vulnerabilities, timeframe for completion and approval of the Mitigation Plan by the CIP Senior Manager.

Summary of all actions described in Part D of the relevant mitigation plan:

Evidence for all milestones will be packaged and uploaded to the Secure Working Folder.

Description of the information provided to [REDACTED] for their evaluation *

Evidence for all milestones will be packaged and uploaded to the Secure Working Folder.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIA Secure Folder and E-MAIL

May 8, 2019

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED] (CIP-007-6 R2)

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-007-6 R2	September 28, 2018

After review for completion on **May 7, 2019**, [REDACTED] staff finds that [REDACTED] has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact [REDACTED]

[REDACTED]


[REDACTED]


Attachment 11

- 11a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-6 R3 submitted May 30, 2018
- 11b. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R3 submitted August 17, 2018
- 11c. The Region's Verification of Mitigation Plan Completion for CIP-007-6 R3 dated May 8, 2019

 This item was signed by [REDACTED] on 5/30/2018



 This item was marked ready for signature by [REDACTED] on 5/30/2018



MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-007-6 R3.	[REDACTED]	[REDACTED]	05/30/2018	Region reviewing Mitigation Plan	Formal	

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name: [REDACTED]

Company Address: [REDACTED]

Compliance Registry ID: [REDACTED]

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name: [REDACTED]

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard: [REDACTED]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R3.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

[REDACTED] "did not implement processes to deter, detect, or prevent malicious code intrusions on certain of its [REDACTED]-based devices. As a result, [Responsible Entity] was not in compliance with the CIP Reliability Standard CIP-007-6 Requirement R3. [REDACTED]

Preliminary assessment revealed two reasons for the possible violation (PV) finding. First, during the time of the audit, the Responsible Entity had a longstanding (from 2010), technically justified internal policy against installing host-based anti-virus solutions on its [REDACTED] systems. Second, personnel managing the [REDACTED] systems during the transition to Version 5 of the CIP Standards overlooked the need to deploy alternative method(s) to detect or prevent malicious code, such as an intrusion detection system (IDS), in the absence of the use of host-based anti-virus solutions.

[Attachments \(\)](#)

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this MitigationPlan:

The eight (8) [REDACTED] servers referenced in the Final Audit Report consist of two (2) PACS servers supporting physical access control to Physical Security Perimeters (PSPs) and six (6) [REDACTED] OS, which are Electronic Access Control Monitoring Systems (EACMS) supporting RSA 2-factor authentication for electronic access to Electronic Security Perimeters (ESPs). As such, the finding involves PACS and EACMS. The Responsible Entity recognizes that CIP-007-6 Requirement R3 does apply to EACMS and PACS, and that Part 3.1 requires alternative method(s) to detect or prevent malicious code in absence of host-based anti-virus solutions, such as an IDS. Indeed, that is what the Responsible Entity has done, as of April 6, 2018, to remediate the finding of non-compliance related to the [REDACTED] servers referenced in the Final Audit Report. As noted, however, for EACMS and PACS, such IDS malicious code solutions can be executed outside of an ESP without running afoul of CIP-007-6 Requirement R3, Part 3.1.

Given the important security objective of protecting Cyber Assets from malicious code and the need for long-term sustainability, representatives from multiple operational Business Units (BUs), [REDACTED] are working collaboratively on the milestone activities in this Mitigation Plan. Personnel from [REDACTED] worked together to develop enterprise-wide program documentation and controls; and, separately, on compliance responsibilities that are managed more effectively with processes, procedures and work templates designed specifically for their BU. The objective of this multi-departmental effort is to create an enterprise-wide program for the Responsible Entity that is consistent across

The BUs are creating enterprise-wide documented processes, work instructions, templates, and controls; developing training programs for all new enterprise-wide documentation; and, will retain all associated implementation evidence throughout execution of the malicious code prevention program. The BUs will document the implementation evidence, evaluating its use throughout the organization, and consolidating where appropriate; and, then finalizing the new enterprise-wide documentation, training, and subsequently implementing a comprehensive enterprise-wide program is expected to take a little less than one (1) year to complete.

Attachments ()

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

- 1: Create an inventory list of policies, standards, procedures, and work instruction documentation for malicious code prevention currently in effect for [REDACTED] Business Units. Inventory list will include document name/number, Business Unit (BU) Owner, and effective date. Completed by September 8, 2017.
- 2: Develop an [REDACTED] inventory list of all existing malicious code prevention implementation evidence templates not previously identified in milestone 1 for [REDACTED] BUs. The output will be an inventory list [REDACTED] templates by name/number, BU Owner, and effective date. Completed by September 8, 2017.
- 3: Determine the sustainability of existing malicious code prevention implementation evidence templates in the inventory list created in milestone 2 for [REDACTED] BUs. Decide 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. The BUs will document what contents and instructions are usable to create enterprise-wide malicious code prevention implementation evidence templates. Completed by September 8, 2017.
- 4: Evaluate the inventory list created in milestone 1 of effective policies, standards, procedures, and work instruction documentation for malicious code prevention for [REDACTED] BUs to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable. The BUs will document what content, instructions, and tools in the policies, standards, procedures, and work instruction documentation for malicious code prevention currently in effect for [REDACTED] is usable and can be combined into corporate-wide documentation. Completed by September 15, 2017.
- 5: Perform an Extent of Condition (EOC). Working with the 1st Quarter 2017 CIP-002 BES Cyber System list, confirm there is documentation based on device type for devices capable of detecting, deterring, or preventing malicious code; and, document how each device is performing (traditional AV, hardening, policies, etc.). If devices use signatures or patterns, or are not capable of malicious code prevention [REDACTED]
- 6: Perform an Extent of Condition (EOC) analysis to identify possible Root Cause(s). The BUs will perform an EOC analysis using the inventory of documentation and devices that were identified during execution of Milestones 1, 2, and 5. The compliance group will compile questions and perform BU SME interviews for additional input for the EOC analysis. The results of the interviews will be given to the BUs to incorporate into the EOC analysis. Possible Root Cause(s) will be identified as a result of the EOC Analysis. Any additional findings of non-compliance will be reported [REDACTED] to the Regional Entities. Completed by October 25, 2017.
- 7: Perform a Root Cause Analysis to determine Root Cause(s) and contributing factor(s). The BUs will perform a Root Cause analysis and identify the root cause(s) and contributing factors. Completed by October 27, 2017.
- 8: Develop a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the Root Cause Analysis. Completed by November 24, 2017.
- 9: Develop a technical and/or procedural solution for those devices that cannot deter, detect or prevent malicious code. This solution should be captured in an enterprise-wide policy document and list the solutions and business justification, (to include vendor documentation, if necessary) for protecting the devices. Completed by December 8, 2017.
- 10: Create enterprise-wide documentation, (which will include input from Milestone 4). The new enterprise-wide documentation should be supplemented with: (A) A process to protect devices from malicious code. This will be based on the assessment performed in Milestone 7, for devices that are not capable of deterring, detecting, or preventing malicious code. BUs will investigate traditional antivirus, system hardening, policies, and use of intrusion detection/prevention devices. (B) Process on how to respond to malicious code detection. Who is this performed by, how alerts for malicious code are setup, how/where should this be documented. (C) Process on how to mitigate the threat of malicious code. After finding possible malicious code and responding, what is the process to restore systems back to normal, safe functions? Who is doing this, and how/where is it documented. (D) Process on how to transition into the Cyber Security Incident Response Plan, if malicious code is detected. (E) Process for the update of signatures or patterns, to include: (i) Who will be performing the update; (ii) How are the updates received; and, (iii) How is testing performed, what does it entail, and how is it documented. (F) How and when to perform installations, for example, is it better to do when installing patches. Completed by December 22, 2017.
- 11: Determine Roles and Responsibilities. Identify ownership of devices by BU to ensure coverage. The BUs will collaboratively determine and document who is responsible for inventoried devices based on location. The BUs will document the responsible BU and the SMEs, Groups, and/or Departments who are responsible for compliance activities for those devices. This exercise will also determine who is responsible for administering training. Completed by December 22, 2017.
- 12: The BUs will develop controls for the CIP-007 processes to make them repeatable and sustainable. Controls for creating and maintaining all processes will be documented for the enterprise-wide documentation developed during the execution of Milestone 10. Completed by January 5, 2018.
- 13: The CIP Senior Manager and BU Directors will review the results of Milestone 5 and agree to their designated BU ownership of devices, and their obligation to maintain processes, evidence and training. A letter will be drafted and signed by the CIP Senior Manager and BU Directors agreeing to assigned compliance responsibilities for specific devices, including training. Completed by January 25, 2018.
- 14: Create enterprise-wide implementation evidence templates for capturing compliance evidence. The templates will have common nomenclature that will be used enterprise-wide. Templates will include: (A) Device name and device type; (B) Which method the device is using to prevent malicious code; (C) If device is not capable of preventing against malicious code, what method is used to protect device; (D) Document if the device uses signatures or patterns; (E) Document when and by whom signatures /patterns have been updated; and, (F) Revision history, proper "Confidential – CEI" headers/footers, columns/fields to capture requirement measures. Completed by February 16, 2018.
- 15: Develop Training program for new and updated documentation and implementation evidence templates. The BUs will develop an enterprise-wide Training program for when documentation and/or implementation evidence templates are created or updated. Personnel listed in the 'Roles and Responsibilities' section of the documentation and implementation evidence templates, and anyone identified as needing the training, will be required to complete the training. Also, each BU will designate who is responsible for administering, maintaining, updating and tracking completion of the training program. Completed by April 6, 2018.
- 16: Perform Training. The BUs will determine 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. Completed by May 18, 2018.
- 17: Implement new and/or updated CIP-007 documentation and controls. BUs will implement the new and/or updated documentation and controls, and submit implementation evidence for each Part of the CIP-007 Requirement R3: (A) Documentation of devices capable of detecting, deterring, or preventing malicious code, and how each device is performing (traditional AV, hardening, policies, etc.). If devices are not capable of malicious code prevention it will also be documented. (B) Document if the devices use signatures or patterns. (C) Document when malicious code is detected, how it is mitigated, what was the response process, and who performed the process. (D) Testing and installation of signature or pattern updates, who they were performed by, and date for testing or update. To be completed by August 17, 2018.

Attachments ()

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

8/17/2018

Implement new and/or updated CIP-007 documentation and controls.

Milestone Pending (Due: 8/17/2018)

Business Units will implement the updated documentation and controls, and submit implementation evidence for each Part of the CIP-007 Requirement R3: (A) Documentation of devices capable of detecting, deterring, or preventing malicious code, and how each device is performing (traditional AV, hardening, policies, etc.). If devices are not capable of malicious code prevention it will also be documented. (B) Document if the devices use signatures or patterns. (C) Document when malicious code is detected, how it is mitigated, what was the response process, and who performed the process. (D) Testing and installation of signature or pattern updates, who they were performed by, and date for testing or update.

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

Given the important security objective of detecting and preventing the introduction of malicious code, the Responsible Entity took a comprehensive approach. [REDACTED] reasons, the Responsible Entity believes that there was, and continues to be, only minimal risk to the reliability of the Bulk Electric System (BES) while the Responsible Entity executes this Mitigation Plan.

The eight (8) [REDACTED] servers referenced in the Final Audit Report consist of two (2) PACS servers supporting physical access control to PSPs through [REDACTED] microcontrollers, and six (6) [REDACTED] OS, which are EACMS supporting RSA 2-factor authentication for electronic access to ESPs. These 8 access and control systems are not used for real time operation of the Bulk Electric System (BES) and would not, even if infected with malicious code, directly impact the reliability operation of the BES. Plus, as of April 6, 2018, the Responsible Entity has now implemented an IDS network level malicious code solution remediating the finding [REDACTED] ce related to the [REDACTED] servers referenced in the Final Audit Report. Malware prevention deficiencies discovered during the Extent of Condition analysis completed October 25, 2017, (see Milestone 6) will be resolved when the Mitigation Plan is complete.

In the meantime, all of the Responsible Entity's Cyber Systems covered by the CIP Reliability Standards will continue to be protected by the company's strong corporate physical and electronic security defense-in-depth posture, as well as controls already implemented for CIP-006-6 Requirements R1 and R2, and CIP-005-5 Require [REDACTED] ctively, these protections greatly reduce any putative risk to the reliability of the BES that may be posed by the lack of malware protection being remediated as part of the Mitigation Plan.

Details on the Responsible Entity's defense-in-depth posture for physical access is set forth in the company's Physical Security Plan for CIP-006-6. As far as electronic access, there are four levels of protection and steps required to remotely access all of the EAPs at the Responsible Entity's High and Medium Impact BES Cyber Systems. Further, all communications and access to EAPs at the Responsible Entity's High Impact Control Center and Medium Impact (Substations' and Generating Facilities') BES Cyber Systems are permitted only through an encrypted network. [REDACTED]

Meanwhile, comparable levels of protection associated with Generation facilities are overseen by plant specific cyber security managers. In sum, an external unauthorized source must bypass multiple layers of firewalls and network protections to gain access to the Responsible Entity's High and Medium Impact BES Cyber Systems.

With regard to risk of malware being introduced remotely to the 8 [REDACTED] servers referenced in the Final Audit Report, an external unauthorized user, (i.e., a user that has not been granted electronic CIP access authorization in accordance with CIP-004-6), would need to successfully navigate the Responsible Entity's 2-factor authentication process to log into a jump server on the corporate network. This is the process that employees and authorized contractors use each day to access the corporate network.

In summary, while the Mitigation Plan is not scheduled to be completed until August 17, 2018, the risk to the reliability of the BES is greatly reduced due to the Responsible Entity's robust defense-in-depth approach to physical and network security.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

By successfully completing this Mitigation Plan, the Responsible Entity will reduce the risk of future alleged violations and ensure compliance by implementing:

- Enterprise-wide documentation with sustainable, repeatable processes and controls for deploying methods to deter, detect, or prevent malicious code;
- Enterprise-wide technical solution documented in a policy for devices that cannot deter, detect, or prevent malicious code;
- A formal training program to ensure all Personnel with documented Roles and Responsibilities are trained on new or updated processes; and,
- Enterprise-wide implementation evidence templates to capture devices that are capable of detecting, deterring, or preventing malicious code; and, how each device is performing, (traditional AV, hardening, policies, etc.), and those devices that use signatures or patterns.

Attachments ()**SECTION F: AUTHORIZATION**

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am [REDACTED]
 - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
 - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric

- I have read and am familiar with the contents of this Mitigation Plan
- [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

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

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED] please contact the [REDACTED] to determine your assigned SPOC at:

[REDACTED]

[REDACTED]

[REDACTED]

This item was signed by [REDACTED] on 8/17/2018

This item was marked ready for signature by [REDACTED] on 8/17/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

Name of Standard of mitigation violation(s):

Requirement	Tracking Number	NERC Violation ID
R3.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

[Implement new and/or updated CIP-007 documentation and controls.](#)

Milestone Completed (Due: 8/17/2018 and Completed 8/17/2018)

[Attachments \(0\)](#)

Business Units will implement the updated documentation and controls, and submit implementation evidence for each Part of the CIP-007 Requirement R3: (A) Documentation of devices capable of detecting, deterring, or preventing malicious code, and how each device is performing (traditional AV, hardening, policies, etc.). If devices are not capable of malicious code prevention it will also be documented. (B) Document if the devices use signatures or patterns. (C) Document when malicious code is detected, how it is mitigated, what was the response process, and who performed the process. (D) Testing and installation of signature or pattern updates, who they were performed by, and date for testing or update.

Summary of all actions described in Part D of the relevant mitigation plan:

Completion Summary and supporting evidence will be uploaded to the Secure Working folder.

Description of the information provided to [REDACTED] for their evaluation *

Completion Summary and supporting evidence will be uploaded to the Secure Working folder.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIA Secure Folder and E-MAIL

May 8, 2019

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED] (CIP-007-6 R3)

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-007-6 R3	August 17, 2018

After review for completion on **May 7, 2019**, [REDACTED] staff finds that [REDACTED] has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact [REDACTED]

[REDACTED]

[REDACTED]

Attachment 12

- 12a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-6 R4 submitted May, 30, 2018
- 12b. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R4 submitted August 17, 2018
- 12c. The Region's Verification of Mitigation Plan Completion for CIP-007-6 R4 dated May 8, 2019

This item was signed by [REDACTED] on 5/30/2018

This item was marked ready for signature by [REDACTED] on 5/30/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation IDs	Date Submitted	Status	Type	Revision Number
CIP-007-6 R4.	[REDACTED]	[REDACTED]	05/30/2018	Region reviewing Mitigation Plan	Formal	

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name:

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard:

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R4.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

[REDACTED] "did not log events of detected malicious code for certain of its [REDACTED] based devices associated with its BES Cyber Systems. As a result, [Responsible Entity] was not in compliance with the CIP Reliability Standard CIP-007-6 Requirement R4. [REDACTED]

The Responsible Entity preliminarily assessed that the reason for the possible violation (PV) finding was that personnel managing the transition to Version 5 of the CIP Standards overlooked the need to deploy security event logging and monitoring solutions for the eight (8) [REDACTED] servers referenced in the Final Audit Report.

Attachments ()

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this Mitigation Plan:

The eight (8) [REDACTED] servers referenced in the Final Audit Report consist of two (2) PACS servers supporting physical access control to PSPs; and, six (6) [REDACTED] OS, which are EACMS supporting RSA 2-factor authentication for electronic access to ESPs. As such, the finding involves PACS and EACMS. EACMS and PACS are not used to operate or control the real time operation of the BES. The Responsible Entity recognizes that CIP-007-6 Requirement R4 requires security event monitoring and logging for EACMS and PACS. To that end, logging of security events for the [REDACTED] servers was implemented on April 6, 2018 to remediate the finding of non-compliance referenced in the Final Audit Report.

Given the important security objective of security event logging and monitoring for all Cyber Assets covered by the CIP Reliability Standards and the need for long-term sustainability, representatives from multiple operational Business Units (BUs) [REDACTED] are working collaboratively on the milestone activities in this Mitigation Plan. Personnel from [REDACTED] worked together to develop enterprise-wide program documentation and controls; and, separately, on compliance responsibilities that are managed more effectively with processes, procedures and work templates designed specifically for their BU. The objective of this multi-departmental effort is to create an enterprise-wide program for the Responsible Entity that is consistent across all BUs, and will facilitate sustainable compliance.

The BUs are creating enterprise-wide documented processes, work instructions, templates, and controls; developing training programs for all new enterprise-wide

[Attachments \(\)](#)

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

- 1: Create an inventory list of policies, standards, procedures, and work instruction documentation for security event monitoring currently in effect for [REDACTED] Business Units. Inventory list will include document name/number, Business Unit (BU) Owner, and effective date. Completed by September 8, 2017.
- 2: Develop an [REDACTED] inventory list of all existing security event monitoring implementation evidence templates not previously identified in milestone 1 for [REDACTED] BUs. The output will be an inventory [REDACTED] evidence templates by name/number, BU Owner, and effective date. Completed by September 8, 2017.
- 3: Determine the sustainability of existing security event monitoring implementation [REDACTED] evidence templates in the inventory list created in milestone 2 for [REDACTED] BUs. Decide how evidence should be structured, and how the security event monitoring implementation evidence templates can be used to create enterprise-wide security event monitoring evidence templates that are repeatable and sustainable. The BUs will document what contents and instructions are usable to create enterprise-wide security event monitoring implementation evidence templates. Completed by September 8, 2017.
- 4: Evaluate the inventory list created in milestone 1 of effective policies, standards, procedures, and work instruction documentation for security event monitoring for [REDACTED] BUs to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable. The BUs will document what content, instructions, and tools in the policies, standards, procedures, and work instruction documentation for security event monitoring currently in effect for [REDACTED] is usable and can be combined into corporate-wide documentation. Completed by September 15, 2017.
- 5: Perform an Extent of Condition (EOC). Working with the 1st Quarter 2017 CIP-002 BES Cyber System list, ensure there is documentation for the devices that are capable of logging and alerting on security events, to include detecting successful login attempts, failed access and login attempts, and malicious code; ensure there is documentation for the devices that can generate alerts for security events [REDACTED] it [REDACTED] review of [REDACTED] October 23, 2017.
- 6: Perform an Extent of Condition (EOC) analysis to identify possible Root Cause(s). The BUs will perform an EOC analysis using the inventory of documentation and devices that were identified during execution of Milestones 1, 2, and 5. The compliance group will compile questions and perform BU SME interviews for additional input for the EOC analysis. The results of the interviews will be given to the BU [REDACTED] incorporate into the EOC analysis. Possible Root Cause(s) will be identified as a result of the EOC Analysis. Any additional findings of non-compliance will be reported to the Regional Entities. Completed by October 25, 2017.
- 7: Perform a Root Cause Analysis to determine Root Cause(s) and contributing factor(s). The BUs will perform a Root Cause analysis and identify the root cause(s) and contributing factors. Completed by October 27, 2017.
- 8: Develop a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the Root Cause Analysis. Completed by November 24, 2017.
- 9: Create enterprise-wide documentation, (which will include input from Milestone 4). The new enterprise-wide documentation will be supplemented with: (A) A process for 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, vendor documentation will be required. (B) A process on generating alerts for security events that require an alert. This includes how the device type generates an alerts, where the alerts go, the format, who reviews, will alerts get pushed to a SIEM, or are they seen by the firewall. (C) A process for retaining event logs for the last 90 consecutive calendar days. This will include who is responsible for this process, where logs will be retained, process for purging old logs, and what will be the reporting process for recording where the logs are kept. In the case of a CIP Exceptional Circumstance event, the process for retaining logs longer than 90 consecutive calendar days. (D) A process on how the BUs determine if a TFE is necessary for when event logs cannot be retained for at least 90 consecutive calendar days. This will include why logs cannot be retained and what compensating measures the BUs have put into place. Process will require using the vendor documentation as evidence. (E) A process for the review of sampled logged events at intervals no greater than 15-calendar days to identify undetected cyber security incidents. The review will include: (i) Name of person performing; (ii) Date of review; (iii) Device type for logged events; (iv) Any findings and how they will be resolved; and (v) Reviewer's signature. (F) Process for suspicious activity that requires activation of the Cyber Security Incident Response Plan. Completed by December 22, 2017.
- 10: Determine Roles and Responsibilities. Identify ownership of devices by BU to ensure coverage. The BUs will collaboratively determine and document who is responsible for inventoried devices based on location. The BUs will document the responsible BU and the SMEs, Groups, and/or Departments who are responsible for compliance activities for those devices. This exercise will also determine who is responsible for administering training. Completed by December 22, 2017.
- 11: The BUs will develop controls for the CIP-007 processes to make them repeatable and sustainable. Controls for creating and maintaining all processes will be documented for the enterprise-wide documentation developed during the execution of Milestone 9. Completed by January 5, 2018.
- 12: The CIP Senior Manager and BU Directors will review the results of Milestone 5 and agree to their designated BU ownership of devices, and their obligation to maintain processes, evidence and training. A letter will be drafted and signed by the CIP Senior Manager and BU Directors agreeing to assigned compliance responsibilities for specific devices, including training. Completed by January 25, 2018.
- 13: Create enterprise-wide implementation evidence templates for capturing compliance evidence. The templates will have common nomenclature that will be used enterprise-wide. Templates will include: (A) Devices that are capable of logging and alerting security events. For logging of events, this includes detection of successful login attempts, failed access and dial-in login attempts, and malicious code. (B) For generating alerts, document which devices are configured to generate alerts for detected malicious code, failure of logging and other events the Responsible Entity deems necessary. (C) Sampling of logged events every 15 calendar days to include who performed the review, any findings from the review, and when the review was completed. (D) Revision history, proper "Confidential – CEII" headers/footers, columns/fields to capture requirement measures. Completed by February 23, 2018.
- 14: Develop Training program for new and updated documentation and implementation evidence templates. The BUs will develop an enterprise-wide Training program for when documentation and/or implementation evidence templates are created or updated. Personnel listed in the 'Roles and Responsibilities' section of the documentation and implementation evidence templates, and anyone identified as needing the training, will be required to complete the training. Also, each BU will designate who is responsible for administering, maintaining, updating and tracking completion of the training program. Completed by April 6, 2018.
- 15: Perform Training. The BUs will determine 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. Completed by May 18, 2018.
- 16: Implement new and/or updated CIP-007 documentation and controls. BUs will implement the new and/or updated documentation and controls and submit implementation evidence for each Part of CIP-007 Requirement R4, to include: (A) List of event types for which the BES Cyber Assets and Systems are capable of detecting and configured to log; (B) List of security events that require alerts, and how alerts are configured for each BES Cyber Asset or System; (C) Evidence of system generated reports for logs being retained for the last 90 consecutive calendar days; and, (D) Documentation of sample entries for performance of review of logged events every 15 calendar days, name of person performing the review, any findings from the review, and date review was completed. To be completed by August 17, 2018.

[Attachments \(\)](#)

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

8/17/2018

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

Milestone Pending (Due: 8/17/2018)

Business Units will implement the new and/or updated documentation and controls and submit implementation evidence for each Part of CIP-007 Requirement R4, to include: (A) List of event types for which the BES Cyber Assets and Systems are capable of detecting and configured to log; (B) List of security events that require alerts, and how alerts are configured for each BES Cyber Asset or System; (C) Evidence of system generated reports for logs being retained for the last 90 consecutive calendar days; and, (D) Documentation of sample entries for performance of review of logged events every 15 calendar days, name of person performing the review, any findings from the review, and date review was completed.

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

Given the important security objective of security event logging and monitoring for all Cyber Assets covered by the CIP Reliability Standards, the Res [REDACTED] [REDACTED] eted by August 17, 2018. For the following reasons, the Responsible Entity believes that there was, and continues to be, only minimal risk to the reliability of the Bulk Electric System (BES) while the Responsible Entity executes this Mitigation Plan.

The eight (8) [REDACTED] servers referenced in the Final Audit Report consist of two (2) PACS servers supporting physical access control to PSPs through [REDACTED] microcontrollers, and six (6) [REDACTED] OS, which are EACMS supporting RSA 2-factor authentication for electronic access to ESPs. These 8 access and control systems are not used for real time operation of the Bulk Electric System (BES) and would not, even if degraded or misused, directly impact the reliability operation of the BES. Plus, as of April 6, 2018, logging and monitoring of security events for the [REDACTED] servers was implemented to remediate the finding of non-compliance [REDACTED] in the Final Audit Report. Logging deficiencies discovered during the Extent of Condition analysis completed October 25, 2017, (see Milestone 6), will be resolved when the Mitigation Plan is complete.

In the meantime, all of the Responsible Entity's Cyber Systems covered by the CIP Reliability Standards will continue to be protected by the company's strong corporate physical and electronic security defense-in-depth posture, as well as controls already implemented for CIP-006-6 Requirements R1 and R2, and CIP-005-5 Requirement [REDACTED]. [REDACTED] ctively, these protections greatly reduce any putative risk to the reliability of the BES that may be posed by the lack of malware protection being remediated as part of the Mitigation Plan.

Details on the Responsible Entity's defense-in-depth posture for physical access is set forth in the company's Physical Security Plan for CIP-006-6. As far as electronic access, there are four levels of protection and steps required to remotely access all of the EAPs at the Responsible Entity's High and Medium Impact BES Cyber Systems. Further, all communications and access to EAPs at the Responsible Entity's High Impact Control Center and Medium Impact (Substations' and Generating Facilities') BES Cyber Systems are permitted only through an encrypted network [REDACTED]

[REDACTED] Meanwhile, comparable levels of protection associated with Generation facilities are overseen by plant specific cyber security managers. In sum, an external unauthorized source must bypass multiple layers of firewalls and network protections to gain access to the Responsible Entity's High and Medium Impact BES Cyber Systems.

With regard to risks posed by the lack of logging and monitoring for the 8 [REDACTED] servers referenced in the Final Audit Report, an external unauthorized user, (i.e., a user that has not been granted electronic CIP access authorization in accordance with CIP-004-6), would need to successfully navigate the Responsible Entity's 2-factor authentication process to log into a jump server on the corporate network. This is the process that employees and authorized contractors use each day to access the corporate network.

In summary, while the Mitigation Plan is not scheduled to be completed until August 17, 2018, the risk to the reliability of the BES is greatly reduced due to the Responsible Entity's robust defense-in-depth approach to physical and network security.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

By successfully completing this Mitigation Plan, the Responsible Entity will have:

- Enterprise-wide documentation with sustainable, repeatable processes and controls for logging and generating alerts for security events;
- A formal training program to ensure all personnel with documented Roles and Responsibilities are trained on the new or updated processes; and,
- Enterprise-wide implementation evidence templates to capture devices that are logging and generating alerts for security events that are reviewed, and investigated, if necessary.

Attachments ()

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am [REDACTED]
 - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
 - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))

- I have read and am familiar with the contents of this Mitigation Plan

- [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

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

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED] please contact the [REDACTED] department to determine your assigned SPOC at:

[REDACTED]

[REDACTED]

[REDACTED]

This item was signed by [REDACTED] on 8/17/2018

This item was marked ready for signature by [REDACTED] on 8/17/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[REDACTED]

Name of Standard of mitigation violation(s):

[REDACTED]

Requirement	Tracking Number	NERC Violation ID
R4.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

[REDACTED]

[Implement new and/or updated CIP-007 documentation and controls.](#)

Milestone Completed (Due: 8/17/2018 and Completed 8/17/2018)

[Attachments \(0\)](#)

Business Units will implement the new and/or updated documentation and controls and submit implementation evidence for each Part of CIP-007 Requirement R4, to include: (A) List of event types for which the BES Cyber Assets and Systems are capable of detecting and configured to log; (B) List of security events that require alerts, and how alerts are configured for each BES Cyber Asset or System; (C) Evidence of system generated reports for logs being retained for the last 90 consecutive calendar days; and, (D) Documentation of sample entries for performance of review of logged events every 15 calendar days, name of person performing the review, any findings from the review, and date review was completed.

Summary of all actions described in Part D of the relevant mitigation plan:

Completion Summary and supporting evidence will be uploaded to the Secure Working folder.

Description of the information provided to [REDACTED] for their evaluation *

Completion Summary and supporting evidence will be uploaded to the Secure Working folder.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIA Secure Folder and E-MAIL

May 8, 2019

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED]

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-007-6 R4	August 17, 2018

After review for completion on **May 7, 2019**, [REDACTED] staff finds that [REDACTED] has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact [REDACTED]

[REDACTED]

[REDACTED]

Attachment 13

- 13a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-3a R5 submitted June 19, 2018
- 13b. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R5 submitted January 2, 2019
- 13c. The Region's Verification of Mitigation Plan Completion for CIP-007-3a R5 dated May 8, 2019

This item was signed by [REDACTED] on 6/19/2018

This item was marked ready for signature by [REDACTED] on 6/19/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-007-6 R5.	[REDACTED]	[REDACTED]	06/19/2018	Region reviewing Mitigation Plan	Formal	

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name:

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard:

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R5.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

[REDACTED] the Responsible Entity "did not properly identify individuals who had authorized access to shared accounts. In addition, [Responsible Entity] did not file a TFE for [a cyber] device, nor demonstrate its implementation of compensating and/or mitigating measures on the [cyber] device(s). As a result, [Responsible Entity] was not in compliance with the CIP Reliability Standard CIP-007-6 Requirement R5. [REDACTED]

Attachments ()

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this Mitigation Plan:

The possible violation (PV) finding has two bases. The first basis, which involves the tracking of individuals with access to shared accounts was addressed as of September 26, 2016, when the Responsible Entity formally created roles for the shared accounts in the company's [REDACTED] and was tracking who had assigned roles to the Active Directory (AD) domain administrator accounts and shared accounts. A gap between [REDACTED] and AD roles was also identified. The [REDACTED] uses [REDACTED] roles to validate a user's business need, training, and PRA. In addition, the [REDACTED] access is managed using an additional in-house application called [REDACTED] which manages privileges for provisioning access to associated assets. Upon further review however, it was discovered that not all Transmission CIP domain groups were identified in the [REDACTED] system. This Mitigation Plan addresses the Responsible Entity's controls for system access, records documentation, and processes for handling default passwords, shared accounts and other generic account types for devices associated with its BES Cyber Systems.

The second basis of the PV finding, wherein the Responsible Entity is faulted for not filing a Technical Feasibility Exception ("TFE"), or implementing compensating measures for a device that could not meet password requirements, is also being addressed by completion of this Mitigation Plan. While the Responsible Entity's compliance group issued written guidance on TFEs under Version 5 of the CIP Reliability Standards, the Responsible Entity lacked a documented process for determining if a TFE is necessary under CIP-007-6 Table R5 – System Access Control for devices that cannot meet the password requirements.

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

- 1: Create an inventory list of policies, standards, procedures, and work instruction documentation for system access control currently in effect for [REDACTED] Business Units. Inventory list will include document name/number, Business Unit (BU) Owner, and effective date. Completed by September 8, 2017.
- 2: Develop an inventory list of all existing system access control implementation evidence templates not previously identified in milestone 1 for [REDACTED] BUs. The output will be an inventory list of the evidence templates by name/number, BU Owner, and effective date. Completed by September 8, 2017.
- 3: [REDACTED] existing [REDACTED] templates in the inventory list created in milestone 2 for [REDACTED] BUs. Decide 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. The BUs will document what contents and instructions are usable to create enterprise-wide system access control implementation evidence templates. Completed by September 8, 2017.
- 4: Evaluate the inventory list created in milestone 1 of effective policies, standards, procedures, and work instruction documentation for system access control for [REDACTED] BUs to determine which content, instructions, and tools meet the Standard requirement and is repeatable and sustainable. The BUs will document what content, instructions, and tools in the policies, standards, procedures, and work instruction documentation for system access control currently in effect for [REDACTED] is usable and can be combined into corporate-wide documentation. Completed by September 15, 2017.
- 5: [REDACTED] Evidence of Condition (EOC). Working with the 1st Quarter 2017 CIP-002 BES Cyber System list, evaluate system access control documentation for each device to validate if there is a method to enforce authentication of interactive user access attempts, or there is business justification documented for infeasibility (Part 5.1); documentation for enabled default or other generic account types that could not be removed, renamed or disabled is available (Part 5.2); individuals who have authorized access to shared accounts have been identified and documented (Part 5.3); records for when known default passwords are changed, or new devices are placed into production; or, documentation or vendor manuals showing that default passwords are randomly, or pseudo-randomly generated and are thereby unique to device (Part 5.4); documentation for those devices, either technically or procedurally, that support password complexity of at least 8 characters in length and 3 or more character types (Part 5.5); records showing for each device with password only authentication, a system-enforced or procedural periodicity is enforced to change passwords every 15-calendar months, or there is a documented business justification for infeasibility (Part 5.6); and, documentation for which devices can limit the number of unsuccessful authentication attempts, or generate alerts after a threshold of unsuccessful authentication attempts occurs (Part 5.7). Completed by October 23, 2017.
- 6: Perform an Extent of Condition (EOC) analysis to identify possible Root Cause(s). The BUs will perform an EOC analysis using the inventory of documentation and devices that were identified during execution of Milestones 1, 2, and 5. The compliance group will compile questions and perform BU SME interviews for additional input for the EOC analysis. The results of the interviews will be given to the BUs to incorporate into the EOC analysis. Possible Root Cause(s) will be identified as a result of the EOC Analysis. Any additional findings of non-compliance will be reported to the Regional Entities. Completed by October 25, 2017.
- 7: Perform a Root Cause Analysis to determine Root Cause(s) and contributing factor(s). The BUs will perform a Root Cause analysis and identify the root cause(s) and contributing factors. Completed by October 27, 2017.
- 8: Develop a list of sustainable countermeasures to the root cause(s) and contributing factors identified during the performance of the Root Cause Analysis. Completed by December 1, 2017.
- 9: Determine Roles and Responsibilities. Identify ownership of devices by BU to ensure coverage. The BUs will collaboratively determine and document who is responsible for inventoried devices based on location. The BUs will document the responsible BU and the SMEs, Groups, and/or Departments who are responsible for compliance activities for those devices. This exercise will also determine who is responsible for administering training. Completed by December 22, 2017.
- 10: Create enterprise-wide documentation, (which will include input from Milestone 4). The new enterprise-wide documentation will be supplemented with the following processes: (A) A method on how interactive user access is authenticated. This process will include: (i) the types, if more than one, of authentication methods used; (ii) individual responsible for process; and, (iii) Individuals identified that are granted interactive user access. (B) A process to determine if a TFE is required for when authentication of interactive user access cannot be enforced. Process will include why this cannot be achieved, what compensating measures the BUs will put into place, and retaining vendor documentation, if applicable. (C) A process to remove, rename or disable default or generic accounts on devices prior to placing into production. This process will include: (i) name of person performing the work; (ii) where confirmation of the account removal is documented and stored; (iii) verification steps; and, (iv) date work performed. (D) A process on documenting shared accounts and the individuals who have authorized access to shared accounts. This process will include adding or replacing CIP devices, or removing a device from production, and how to remove that device and shared account information from implementation evidence template. (E) A process for changing default passwords on devices prior to being placed into production. If password cannot be changed and is unique to the device, then the process shall state this and require that vendor documentation be maintained as evidence. (F) Process for enforcing password complexity, by determining whether technically or procedurally passwords are enforced based on device type. (G) Process for enforcing password changes at least once every 15 calendar months. (H) Process to determine if a TFE is required for when passwords cannot be changed on specific devices or device types every 15 calendar months. Process will include documenting why this cannot be achieved and what compensating measures the BUs put into place, and maintaining vendor documentation, if applicable. (I) Process on how devices shall limit the number of unsuccessful authentication attempts, or generate alerts after a threshold of unsuccessful authentication attempts occurs. (J) If devices are not capable of limiting the number of unsuccessful authentication attempts, or generating alerts after a threshold of unsuccessful authentication attempts, then document how the BU shall determine if a TFE is necessary. Process will include why this cannot be achieved, what compensating measures the BUs will put into place, and retaining vendor documentation, if applicable. Completed by January 12, 2018.
- 11: The BUs will develop 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. Completed by January 19, 2018.
- 12: The CIP Senior Manager and BU Directors will review the results of Milestone 5 and agree to their designated BU ownership of devices, and their obligation to maintain processes, evidence and training. A letter will be drafted and signed by the CIP Senior Manager and BU Directors agreeing to assigned compliance responsibilities for specific devices, including training. Completed by January 25, 2018.
- 13: Create enterprise-wide implementation evidence templates for capturing compliance evidence. The templates will have common nomenclature that will be used enterprise-wide. Templates will include: (A) Device name and device type; (B) Which method the device uses to authenticate user access; (C) If device is able to limit the number of unsuccessful authentication attempts, or generate alerts after a threshold of unsuccessful authentication attempts occur; (D) If device has a default password, or allows for password complexity; (E) Document password capabilities, compensating measures, and location of stored vendor documentation; and, (F) Revision history, proper "Confidential – CEII" headers or footers, columns or fields to capture requirement measures. Completed by February 16, 2018.
- 14: Review and validate that all Active Directory (AD) groups in the [REDACTED] have properly assigned roles. Verify that all CIP AD roles in the [REDACTED] have a corresponding access management role, that all [REDACTED] access management roles are found in [REDACTED] and that all [REDACTED] administrators have a corresponding access management role. Completed by February 16, 2018.
- 15: Move all [REDACTED] access from [REDACTED] to [REDACTED]. Using the results of milestone 14, create new [REDACTED] roles to migrate all CIP [REDACTED] access currently in [REDACTED] and ensure new roles require both PRA and NERC CIP Training, assign authorized individuals the new [REDACTED] roles, remove all AD CIP access from [REDACTED] and create an access matrix to maintain all roles. Completed by March 9, 2018.
- 16: Identify how the Access Control Lists (ACL) are determined across the various platform types. Contact the SMEs for each CIP device and solicit documentation on each platform's ACL. Gather the requirements needed to extract the ACL data from target systems. Completed by March 23, 2018.
- 17: Develop Training program for new and updated documentation and implementation evidence templates. The BUs will develop an enterprise-wide Training program for when documentation and/or implementation evidence templates are created or updated. Personnel listed in the 'Roles and Responsibilities' section of the documentation and implementation evidence templates, and anyone identified as needing the training, will be required to complete the training. Also, each BU will designate who is responsible for administering, maintaining, updating and tracking completion of the training program. Completed by April 6, 2018.
- 18: Perform Training. The BUs will determine 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. Completed by May 18, 2018.
- 19: Perform an Extent of Condition (EOC) by identifying all CIP non-Windows devices, and mapping all roles from the CIP non-Windows device to the access management

system roles in [REDACTED] Verify that access to CIP non-Windows 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 Regional Entities of any compliance issues discovered. To be completed by June 2, 2018.

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

20: Create a standardized enterprise-wide access matrix template with clearly defined roles. Working with the results of milestones 16 and 19, identify the enterprise-wide access matrix requirements, (including how privileges must be captured), create a roles guideline (rules on what makes up a role and how roles should be used), and determine the feasibility of consolidating into one enterprise-wide list. To be completed by August 1, 2018.

21: Implement countermeasures and execute updated CIP-007 documents and controls. The BUs will implement the updated documents and controls, and submit implementation evidence for each part of CIP-007-6 Requirement R5, which will include: (A) Documentation describing how interactive user access is authenticated; (B) List of known enabled default or other generic account types for each device; (C) List of shared accounts and individuals who have authorized access for each device or device type; (D) Evidence that known default passwords were changed, per cyber asset capability, for each device. This will include date password was changed and by whom. (E) System generated reports or screenshots from devices that enforce password parameters for length and complexity. (F) System generated reports, screenshots or attestations for devices that demonstrate passwords were changed every 15-calendar months. (G) Documentation for the devices that limit the number of unsuccessful authentication attempts or generate alerts, and any rules for configuring the alerting. To be completed by August 17, 2018.

22: Develop a mechanism for extracting and comparing the access management tool's users and roles to target system's Access Control List (ACL). Identify the new process and/or tool to be used to extract target system's ACLs, and identify the new process and/or tool that will be used to compare the extracted ACLs to the access management tool's authorized users. To be completed by September 30, 2018.

23: Perform an Extent of Condition (EOC) by identifying all CIP Windows devices, and mapping all roles from the CIP Windows device to the access management system roles in [REDACTED]. Verify that access to CIP Windows 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. To be completed by October 5, 2018.

24: Clean-up and restructure roles. Using the results of previous milestones, clean-up and/or restructure roles by removal, modification or creation of 'new' roles. To be completed by October 30, 2018.

25: Enterprise-wide Access Matrix. Create a new enterprise-wide access matrix, and populate with roles. To be completed by December 31, 2018.

Attachments ()

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

12/31/2018

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

Create Standardized Enterprise-wide Access Matrix Template

Milestone Pending (Due: 8/1/2018)

Create a standardized enterprise-wide access matrix template with clearly defined roles. Working with the results of milestones 16 and 19, identify the enterprise-wide access [REDACTED] requirements, (including how privileges must be captured), create a roles guideline (rules on what makes up a role and how roles should be used), and determine the feasibility of consolidating into one enterprise-wide list.

Implement countermeasures and execute updated CIP-007 documents and controls.

Milestone Pending (Due: 8/17/2018)

The BUs will implement the updated documents and controls, and submit implementation evidence for each part of CIP-007-6 Requirement R5, which will include: (A) Documentation describing how interactive user access is authenticated; (B) List of known enabled default or other generic account types for each device; (C) List of shared accounts and individuals who have authorized access for each device or device type; (D) Evidence that known default passwords were changed, per cyber asset capability, for each device. This will include date password was changed and by whom. (E) System generated reports or screenshots from devices that enforce password parameters for length and complexity. (F) System generated reports, screenshots or attestations for devices that demonstrate passwords were changed every 15-calendar months. (G) Documentation for the devices that limit the number of unsuccessful authentication attempts or generate alerts, and any rules for configuring the alerting.

Mechanism for Extracting and Comparing Users and Roles

Milestone Pending (Due: 9/28/2018)

Develop a mechanism for extracting and comparing the access management tool's users and roles to target system's Access Control List (ACL). Identify the new process [REDACTED] tool to be used to extract target system's ACLs, and identify the new process and/or tool that will be used to compare the extracted ACLs to the access management tool's authorized users.

Extent of Condition (EOC)

Milestone Pending (Due: 10/5/2018)

Perform an Extent of Condition (EOC) by identifying all CIP Windows devices, and mapping all roles from the CIP Windows device to the access management system roles in [REDACTED]. Verify that access to CIP Windows 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.

Clean-up and Restructure Roles

Milestone Pending (Due: 10/30/2018)

Using the results of previous milestones, clean-up and/or restructure roles by removal, modification or creation of 'new' roles.

Enterprise-wide Access Matrix

Milestone Pending (Due: 12/31/2018)

Create a new enterprise-wide access matrix, and populate with roles.

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

The second distinct category covered in this Mitigation Plan covers electronic access to BES Cyber Systems. The Responsible Entity decided it needed to thoroughly examine the multiple systems used within the organization to identify and manage individuals with electronic access to Cyber Assets. The Responsible Entity utilizes an [REDACTED] and [REDACTED] to manage electronic access. It concluded the best a [REDACTED] develop a comprehensive Mitigation Plan that would essentially investigate and assess each system's configurations for input, output, tracking, reporting, accuracy and ease-of-use for managing user access to Cyber Assets.

Despite the deficiencies highlighted in the final audit report, the risk to the reliability of the BES is minimal during the execution phase of this Mitigation Plan as the Responsible Entity's BES Cyber Systems will continue to be protected by strong physical and electronic security defense-in-depth controls that have been implemented in accordance with NERC CIP-006-6 Requirements R1 and R2, and CIP-005-5 Requirement R2. Four levels of protection and steps are required in order to remotely access all of the Electronic Access Points (EAPs) at the Responsible Entity's High and Medium Impact BES Cyber Systems. Further, all communications and access to EAPs at the Responsible Entity's Control Center High and Medium Impact BES Cyber Systems are permitted only through an encrypted network.

Meanwhile, comparable levels of protection for Medium Impact BES Cyber Systems associated with Generation facilities are overseen by plant specific cyber security managers. In sum, an external unauthorized source must bypass multiple layers of firewalls and network protections to take advantage of, or exploit, generic passwords or similar vulnerabilities associated with the Responsible Entity's High and Medium Impact BES Cyber Systems.

Collectively, these protections greatly reduce any putative risk to the reliability of the BES that may be posed by the PV finding. Nevertheless, the Responsible Entity's Business Units (BUs) are aware of the security risk posed by inadequate controls for system access, and undocumented records and processes for handling default passwords, shared accounts and other generic account types for devices associated with its BES Cyber Systems. By completing all milestones in this Mitigation Plan, the Responsible Entity expects to greatly minimize any risk the PV finding may be deemed to pose to the BES and ensure that a sustainable program is in place to cover all Parts of Requirement R5. In the meantime, as noted above, the risk to the reliability of the BES is greatly reduced due to the Responsible Entity's robust defense-in-depth approach to physical and network security.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

By successfully completing this Mitigation Plan, the Responsible Entity will reduce the risk of future alleged violations and ensure compliance by having implemented:

- Enterprise-wide documentation that is sustainable, with repeatable processes and controls for system access;
- Access Management Control Matrix that is maintained by understanding all current access roles, new access methodologies, and continuously redefining access roles around the new methodologies
- A documented training program to ensure all Personnel with documented Roles and Responsibilities are trained on the new or updated processes and procedures; and,
- Enterprise-wide implementation evidence templates to capture for each device or device type:
 - Interactive user-access authentication;
 - Enabled default or generic accounts;
 - Shared accounts and all individuals with access to those accounts;
 - Change to default passwords;
 - Enforcing password length and complexity;
 - Password changes once every 15-calendar months; and,
 - Limiting the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful authentication attempts has occurred.

Attachments ()

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am [REDACTED]
 - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
 - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
 - I have read and am familiar with the contents of this Mitigation Plan
 - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED] please contact the [REDACTED] department to determine your assigned SPOC at:

Response	Percentage
Yes, the current system is the best way to run the country	65%
No, the current system is not the best way to run the country	35%

This item was signed by [REDACTED] on 1/2/2019

This item was marked ready for signature by [REDACTED] on 12/31/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

Name of Standard of mitigation violation(s):

Requirement	Tracking Number	NERC Violation ID
R5.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

[Create Standardized Enterprise-wide Access Matrix Template](#)

Milestone Completed (Due: 8/1/2018 and Completed 7/31/2018)

[Attachments \(0\)](#)

Create a standardized enterprise-wide access matrix template with clearly defined roles. Working with the results of milestones 16 and 19, identify the enterprise-wide access [REDACTED] requirements, (including how privileges must be captured), create a roles guideline (rules on what makes up a role and how roles should be used), and determine the feasibility of consolidating into one enterprise-wide list. [REDACTED]

[Implement countermeasures and execute updated CIP-007 documents and controls.](#)

Milestone Completed (Due: 8/17/2018 and Completed 8/17/2018)

[Attachments \(0\)](#)

The BUs will implement the updated documents and controls, and submit implementation evidence for each part of CIP-007-6 Requirement R5, which will include: (A) Documentation describing how interactive user access is authenticated; (B) List of known enabled default or other generic account types for each device; (C) List of shared accounts and individuals who have authorized access for each device or device type; (D) Evidence that known default passwords were changed, per cyber asset capability, for each device. This will include date password was changed and by whom. (E) System generated reports or screenshots from devices that enforce password parameters for length and complexity. (F) System generated reports, screenshots or attestations for devices that demonstrate passwords were changed every 15-calendar months. (G) Documentation for the devices that limit the number of unsuccessful authentication attempts or generate alerts, and any rules for configuring the alerting.

[Mechanism for Extracting and Comparing Users and Roles](#)

Milestone Completed (Due: 9/28/2018 and Completed 9/28/2018)

[Attachments \(0\)](#)

Develop a mechanism for extracting and comparing the access management tool's users and roles to target system's Access Control List (ACL). Identify the new process [REDACTED] tool to be used to extract target system's ACLs, and identify the new process and/or tool that will be used to compare the extracted ACLs to the access management tool's authorized users. [REDACTED]

[Extent of Condition \(EOC\)](#)

Milestone Completed (Due: 10/5/2018 and Completed 10/5/2018)

[Attachments \(0\)](#)

Perform an Extent of Condition (EOC) by identifying all CIP Windows devices, and mapping all roles from the CIP Windows device to the access management system roles in [REDACTED]. Verify that access to CIP Windows 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.

[Clean-up and Restructure Roles](#)

Milestone Completed (Due: 10/30/2018 and Completed 10/30/2018)

[Attachments \(0\)](#)

Using the results of previous milestones, clean-up and/or restructure roles by removal, modification or creation of 'new' roles.

[Enterprise-wide Access Matrix](#)

Milestone Completed (Due: 12/31/2018 and Completed 12/31/2018)

[Attachments \(0\)](#)

Create a new enterprise-wide access matrix, and populate with roles.

Summary of all actions described in Part D of the relevant mitigation plan:

Milestones 1 through 25 are complete; and, the evidence for all mitigating actions has been uploaded to the Secure Working folder.

Description of the information provided to [REDACTED] for their evaluation *

Milestones 1 through 25 are complete; and, the evidence for all mitigating actions has been uploaded to the Secure Working folder.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIA Secure Folder and E-MAIL

May 8, 2019

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED] (CIP-007-6 R5)

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-007-6 R5	January 2, 2019

After review for completion on **May 7, 2019**, [REDACTED] staff finds that [REDACTED] has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact [REDACTED]

[REDACTED]

[REDACTED]

Attachment 14

- 14a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-010-2 R2 submitted May 23, 2018
- 14b. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R2 submitted May 29, 2018
- 14c. The Region's Verification of Mitigation Plan Completion for CIP-010-2 R2 dated October 24, 2018

This item was signed by [REDACTED] on 5/23/2018

This item was marked ready for signature by [REDACTED] on 5/23/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-010-2 R2.	[REDACTED]	[REDACTED]	05/23/2018	Region reviewing Mitigation Plan	Formal	

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name: [REDACTED]

Company Address: [REDACTED]

Compliance Registry ID: [REDACTED]

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name: [REDACTED]

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard: [REDACTED]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R2.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

[REDACTED] "did not have documented processes for investigating detected unauthorized changes to baseline configurations of its BES Cyber Assets" (p.22). At the same time, the report acknowledges that the Responsible Entity had procedures in place for monitoring High Impact BES Cyber Systems and their associated Electronic Access Control and Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) configurations for changes every 35 days or less. Likewise, the report notes that an automated "remedy ticket" would be created in the event of an unauthorized configuration change.

"Audit staff found that while [Responsible Entity's] processes provide for the monitoring of configuration changes and documenting such changes, the processes did not include actions or procedures that should be implemented by the company to initiate and conduct investigations of unauthorized configuration changes. By not having established investigation procedures the company failed to comply with this requirement" (p.23).

[Attachments \(\)](#)

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this MitigationPlan:

[REDACTED] Given the important security objective of investigating and properly documenting unauthorized configuration changes, the Responsible Entity completed this Mitigation Plan in a timely and thorough manner to minimize the likelihood of future similar possible non-compliance findings.

[Attachments \(\)](#)

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake on which it undertook if this Mitigation Plan has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

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

- 0: Upon preliminarily assessing the root cause of the PV finding, it was determined that the Responsible Entity's implemented processes did not include explicit investigative procedures to follow in the event of unauthorized configuration changes that triggered the creation of a remedy ticket. Completed by August 1, 2017.
- 1: Perform an Extent of Condition Analysis. Identify all procedures for High Impact BCS within the Responsible Entity that require enhancements to include the process for documenting and investigating detected unauthorized changes. Completed by October 27, 2017.
- 2: Develop narrative for enhancements by scripting the specific steps to be performed by Subject Matter Experts when baseline inconsistencies are observed. Completed by November 24, 2017.
- 3: Incorporate the enhancements developed in Milestone No. 2, including the creation of new controls, into the CIP-010 Procedures for High Impact BCS. Ensure linkages are established to other relevant Cyber Security Policies and Procedures. Completed by December 29, 2017.
- 4: Obtain and document the required approvals and sign-offs of revised documentation before training. (Ensure effective date for updated documentation is post-training completion date.) Completed by January 12, 2018.
- 5: Schedule and administer training to those individuals within the Responsible Entity who perform the tasks covered by the procedures. Training will be designed to sustain ongoing content updates, tracking and delivery. Completed by January 24, 2018.
- 6: Communicate and disseminate documentation enterprise-wide by notifying impacted personnel of updates to documentation. Ensure new documentation is posted on SharePoint and related previous versions of documentation are retired. Completed by January 31, 2018.
- 7: Correct for any deficiencies found while completing the previous milestones. Utilizing all new or updated policies, procedures, work instructions and/or training, mitigate for any deficiencies identified during the completion of previous milestones. Additionally, any changes to, additions or deletions of BCS assets from the initial 1st Quarter 2017 CIP-002 BES Cyber System lists will be identified, and if necessary, mitigated per new or updated policies, procedures, work instructions and/or training. Completed by February 28, 2018.

Attachments ()

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

2/28/2018

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

No Milestones Defined

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

With regard to risk, the Possible Violation (PV) finding involves the lack of sufficiently documented processes for investigating unauthorized baseline configuration changes to High Impact BES Cyber Systems. However, despite the putative seriousness of any deficiency involving High Impact BES Cyber Systems, the Responsible Entity believes that the actual risk posed to the reliability of the BES was low to non-existent while this Mitigation Plan was being implemented.

Based on a review of all recorded incident tickets reported to the [REDACTED] there is no evidence to indicate that there has been any instance of an unauthorized change to a baseline configuration since the July 1, 2016 effective date of this requirement; and, January 31, 2018, when training had been completed and the updated procedures were officially implemented.

Although the PV in the Final Audit Report was not fully mitigated until January 31, 2018, there was very little risk that unauthorized changes to the baseline configuration would occur. (Of note, the Mitigation Plan was scheduled for completion by February 28, 2018. The final mitigating action was to correct for any deficiencies found during execution of previous milestone activities, of which there were none.) CIP Reliability Standard CIP-010-2, Requirement R2 applies to High Impact BES Cyber Assets, which are protected by physical access protection, data segregation, and access controls. These BES Cyber Assets are protected by many defenses, including firewalls and network protections that would need to be bypassed before an external source could obtain the access necessary to implement a baseline configuration change.

Further, even assuming an unauthorized baseline configuration change was made at a High Impact BES Cyber Asset, the Responsible Entity's system automatically monitors and alerts the SME/device owner of any detected variations in the baseline. The Responsible Entity's monitoring system produces automated remedy tickets that are investigated by the SME/device owner and, if necessary, resolved by the [REDACTED] pursuant to the Responsible Entity's Cyber Security Incident Response Procedure. Thus, regardless of whether the Responsible Entity's written procedure documents the steps to initiate and complete an investigation, there was little to no risk that an unauthorized change in a baseline configuration would not be detected and investigated.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

[REDACTED] res to follow in the event that an unauthorized change to a baseline configuration is detected. SMEs will be trained on how to conduct a proper investigation; and, how to complete the evidence documentation for the investigation. The implemented procedures will provide a sustainable process for when an unauthorized change to a baseline configuration is detected.

Attachments ()

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am [REDACTED]

- I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
- I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
- I have read and am familiar with the contents of this Mitigation Plan
- [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned [REDACTED] single point of contact (SPOC).

If you do not know your assigned [REDACTED] please contact the [REDACTED] ation department to determine your assigned SPOC at:

[REDACTED]

[REDACTED]

[REDACTED]

This item was signed by [REDACTED] on 5/29/2018

This item was marked ready for signature by [REDACTED] on 5/29/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[REDACTED]

Name of Standard of mitigation violation(s):

[REDACTED]

Requirement	Tracking Number	NERC Violation ID
R2.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

[REDACTED]

No Milestones Defined

Summary of all actions described in Part D of the relevant mitigation plan:

Completion Summaries for all milestones have been uploaded to the Secure Working folder.

Description of the information provided to [REDACTED] for their evaluation *

Completion Summaries for all milestones have been uploaded to the Secure Working folder.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIA Secure Folder and E-MAIL

October 24, 2018

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED] (CIP-010-2 R2)

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-010-6 R2	May 23, 2018

After review for completion on **October 24, 2018**, [REDACTED] staff finds that [REDACTED]
has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this
mitigation plan.

If you have any questions, please feel free to contact [REDACTED]

[REDACTED]

[REDACTED]

Attachment 15

- 15a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-011-2 R1 submitted May 23, 2018
- 15b. The Entity's Certification of Mitigation Plan Completion for CIP-011-2 R1 submitted May 31, 2018
- 15c. The Region's Verification of Mitigation Plan Completion for CIP-011-2 R1 dated May 18, 2019

This item was signed by [REDACTED] on 5/23/2018

This item was marked ready for signature by [REDACTED] on 5/23/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-011-2 R1.	[REDACTED]	[REDACTED]	01/02/2018	Revision Requested	Formal	
CIP-011-2 R1.	[REDACTED]	[REDACTED]	05/23/2018	Region reviewing Mitigation Plan	Formal	1

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name:

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard:

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R1.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

[REDACTED] a Storage Area Network (SAN) used to store automated baseline and security configurations for BES Cyber Assets was not properly identified as a BES Cyber System Information (BCSI) Storage Location (p.23-24). The automated baseline configuration software is used for change control management for some of the BES Cyber Assets used at the RE's control center [REDACTED]. The auditors noted that although the RE had a clear description of what information should be identified as BCSI, the RE lacked a documented process or procedure for its employees and relied solely on employee training. The report concluded that the RE should have a formal documented process or procedure that clearly explains BCSI and how it should be handled, labeled, and stored.

[Attachments \(\)](#)

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this MitigationPlan:

The Responsible Entity uses a commercial off-the-shelf solution for retrieval of baseline configurations, which includes security configurations. The servers that store the security configurations are connected to the local SAN server identified in the report which was not properly identified as a BCSI Storage Location. The servers with the commercial off-the-shelf solution however, are housed within a secured data cabinet which requires badge reader access.

[Attachments \(\)](#)

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to take to implement the Mitigation Plan. If the Mitigation Plan has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

1: For the cited BES Cyber System Information (BCSI) Storage Location, determine if there is a related access role in the [REDACTED] for the storage location cited, and document the evidence if the role exists in [REDACTED]. If there is no access role in [REDACTED] for this location, create a role to ensure the location is properly identified as a BCSI Storage Location with access controls. Perform a risk assessment to fully understand the BES risk for the Responsible Entity and the Reliability Coordinator. Completed by October 12, 2017.

2: Perform an Extent of Condition (EOC) Analysis to (1) Identify any BCSI Storage Locations that have not been properly identified; and, (2) Identify and document the existence of any unknown additional root causes. Report to compliance organization any BCSI Storage Locations found that have not been properly identified. Completed by December 4, 2017.

3: Perform Root Cause Analysis to (1) Identify possible root cause(s) for the storage location not being properly identified; and, (2) Verify the root cause(s) by identifying and validating the contributing factors. Completed by December 7, 2017.

4: Develop list of countermeasures leveraging results from the Root Cause Analysis; and, develop 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) [REDACTED]

[REDACTED] Completed by December 20, 2017.

5: Address any EOC findings by: (1) Creating any necessary additional [REDACTED] access roles for any BCSI Storage Location(s) identified; (2) Assign access to any new storage locations identified; and, (3) Properly classify and label the electronic and/or physical documents for any new storage locations identified. Completed by January 22, 2018.

6: Implement countermeasures for enterprise-wide methodology to identify BCSI. (1) Using countermeasures identified in previous milestones, create and/or revise processes documentation to ensure there is an explicit methodology for identifying existing and new electronic and/or physical BCSI: (a) The updated, new methodology needs to clearly address how to identify and/or create both electronic and physical repositories (storage); (b) New methodology and supporting procedures will be sustainable and also address use, handling, transit of BCSI (new and existing); and, (c) Needs to follow NERC guidelines for protecting sensitive information; plus, (2) Obtain approvals for the new and revised enterprise-wide documentation (methodology and procedures) that encompass the IPP: (a) Obtain required approvals and sign-offs for revised documents before training; and, (b) Ensure effective date for updated documents is post-training completion date. Completed by February 26, 2018.

7: Update and deliver training. (1) Develop 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, and, (2) Schedule and administer training, at a minimum, for all users across all Business Units with access to approved BCSI Storage Locations. (Note: Procedures should 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.) Completed by March 26, 2018.

8: Communicate and disseminate newly revised IPP documentation enterprise-wide by: (1) Notifying impacted personnel of the documentation updates; and (2) Ensuring that all new, revised documentation is posted on SharePoint and related previous documents are retired. Completed by April 25, 2018.

Attachments ()

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

4/25/2018

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

Address any EOC findings related to high/medium impact BES Cyber Systems

Milestone Completed (Due: 1/22/2018 and Completed 1/22/2018)

1. Create any necessary additional [REDACTED] access roles for any BCSI storage location(s) identified in the EOC
2. Assign access to any new storage locations identified
3. Properly classify and label the electronic and/or physical documents for any new storage locations identified in the EOC

Implement countermeasures for enterprise-wide methodology to identify BCSI

Milestone Completed (Due: 2/26/2018 and Completed 2/26/2018)

1. Using countermeasures identified in previous milestones, create and/or revise process documentation to ensure there is an explicit methodology for identifying existing and new electronic and/or physical BCSI that must be protected.
 - a. The updated, new methodology needs to clearly address how to identify and/or create both electronic and physical repositories (storage)
 - b. New methodology and supporting procedures will be sustainable and also address use, handling, and transit of BCSI (new and existing)
 - c. The new methodology needs to follow NERC guidelines for protecting sensitive information (also identified in previous milestone)
2. Obtain approvals for the new and revised enterprise-wide documentation (methodology and procedures) that encompass the IPP
 - a. Obtain required approvals and sign-offs for revised documents before training
 - b. Ensure effective date for updated documents is post-training completion date

Update & Deliver Training

Milestone Completed (Due: 3/26/2018 and Completed 3/26/2018)

1. Develop 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.
2. Schedule and administer training, at a minimum, for all users across all BUs with access to approved [REDACTED] BCSI storage locations.
(Note - Procedures documented should indicate that IPP training is to be performed annually, and is also to be provided for new personnel that will be having access to BCSI and/or any BCSI storage locations.)

Communicate deployment

Milestone Completed (Due: 3/30/2018 and Completed 4/25/2018)

Communicate and disseminate newly revised IPP documents across the enterprise

1. Notify impacted personnel of the documentation update
2. Ensure that all new, revised documents are posted on SharePoint and related previous revisions of documents are retired.

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information

may be provided as an attachment):

The risk presented by the possible violation (PV) finding is the risk of unauthorized access to BCSI residing in the storage area network for the application, which includes baseline and security configuration data for High Impact BES Cyber Assets in the System Control Center. Despite the putative seriousness of this risk, for the following reasons, the actual risk to the reliability of the BES remained low while this Mitigation Plan was being implemented and completed by April 25, 2018.

As part of its Mitigation Plan, the Responsible Entity also undertook an extent of condition to review all High and Medium Impact Bulk Electric System (BES) Cyber Systems and identify any storage locations that had not been properly identified as BCSI Storage Locations. This extent of condition, which was completed on December 4, 2017, did not identify any storage locations that had not been properly identified as BCSI Storage Locations. Thus, the SAN server identified in the audit was the only storage location the Responsible Entity failed to properly identify as a BCSI Storage Location and this deficiency had been remediated as part of the Responsible Entity's Mitigation Plan.

For the foregoing reasons, the risk to the reliability of the BES remained low while this Mitigation Plan was being implemented and completed on April 25, 2018.

[Attachments \(\)](#)

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

an updated methodology, and comprehensive program documentation for identifying, labeling, storing, and protecting BCSI. Completion of the Mitigation Plan will ensure that appropriate protections are applied through training, communication and dissemination of the updated methodology and supporting program documentation. Refresher training courses will also be conducted on the Responsible Entity's website will be communicated to personnel to prevent reoccurrence. The methodology and comprehensive program documentation will be an integral part of the Company's Information Protection Program (IPP). The controls will be sustained through annual validations and refresher training courses, which will be regularly communicated and accessible to personnel to ensure consistent and continuous application and use.

[Attachments \(\)](#)

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am
 - I am qualified to sign this Mitigation Plan on behalf of
 - I understand obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
 - I have read and am familiar with the contents of this Mitigation Plan
 - agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned single point of contact (SPOC).

If you do not know your assigned please contact the department to determine your assigned SPOC at:

This item was signed by [REDACTED] on 5/31/2018

This item was marked ready for signature by [REDACTED] on 5/31/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

Name of Standard of mitigation violation(s):

Requirement	Tracking Number	NERC Violation ID
R1.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

Address any EOC findings related to high/medium impact BES Cyber Systems

Milestone Completed (Due: 1/22/2018 and Completed 1/22/2018)

[Attachments \(0\)](#)

1. Create any necessary additional EAMS access roles for any BCSI storage location(s) identified in the EOC
2. Assign access to any new storage locations identified
3. Properly classify and label the electronic and/or physical documents for any new storage locations identified in the EOC

Implement countermeasures for enterprise-wide methodology to identify BCSI

Milestone Completed (Due: 2/26/2018 and Completed 2/26/2018)

[Attachments \(0\)](#)

1. Using countermeasures identified in previous milestones, create and/or revise process documentation to ensure there is an explicit methodology for identifying existing and new electronic and/or physical BCSI that must be protected.
 - a. The updated, new methodology needs to clearly address how to identify and/or create both electronic and physical repositories (storage)
 - b. New methodology and supporting procedures will be sustainable and also address use, handling, and transit of BCSI (new and existing)
 - c. The new methodology needs to follow NERC guidelines for protecting sensitive information (also identified in previous milestone)
2. Obtain approvals for the new and revised enterprise-wide documentation (methodology and procedures) that encompass the IPP
 - a. Obtain required approvals and sign-offs for revised documents before training
 - b. Ensure effective date for updated documents is post-training completion date

Update & Deliver Training

Milestone Completed (Due: 3/26/2018 and Completed 3/26/2018)

[Attachments \(0\)](#)

1. Develop 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.
2. Schedule and administer training, at a minimum, for all users across all BUs with access to approved [REDACTED] BCSI storage locations.
(Note - Procedures documented should indicate that IPP training is to be performed annually, and is also to be provided for new personnel that will be having access to BCSI and/or any BCSI storage locations.)

Communicate deployment

Milestone Completed (Due: 3/30/2018 and Completed 4/25/2018)

[Attachments \(0\)](#)

Communicate and disseminate newly revised IPP documents across the enterprise

1. Notify impacted personnel of the documentation update
2. Ensure that all new, revised documents are posted on SharePoint and related previous revisions of documents are retired.

Summary of all actions described in Part D of the relevant mitigation plan:

The Completion Summaries and all supporting evidence for Milestones 1 through 8 were uploaded to the Secure Working folder.

Description of the information provided to [REDACTED] for their evaluation *

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

The Completion Summaries and all supporting evidence for Milestones 1 through 8 were uploaded to the Secure Working folder.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIA Secure Folder and E-MAIL

May 8, 2019

Re: [REDACTED]
Mitigation Plan Verification of Completion
[REDACTED] (CIP-011-2 R1)

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-011-2 R1	May 31, 2018

After review for completion on **May 7, 2019**, [REDACTED] staff finds that [REDACTED] has completed this Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact [REDACTED]

[REDACTED]

[REDACTED]

Attachment 16

- 16a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-005-3a R2 submitted January 26, 2015**
- 16b. The Entity's Certification of Mitigation Plan Completion for CIP-005-3a R2 submitted December 17, 2015**
- 16c. The Region's Verification of Mitigation Plan Completion for CIP-005-3a R2 dated October 25, 2016**

This item was signed by [REDACTED] on 1/26/2015

This item was marked ready for signature by [REDACTED] on 1/26/2015

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name:

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard:

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R2.	[REDACTED]	[REDACTED]	[REDACTED]

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

[REDACTED] the RE uses an access control model such that explicit access permissions are specified.

Several examples within the provided configuration files for the Access Points illustrate access rules for greater than [REDACTED] hosts (for example IP addresses that allows the last octet set to zero for either source or destination), and in some cases [REDACTED] networks (for example IP addresses allowing the last 2 octets set to zero for either source or destination), this [REDACTED] in many cases beyond the total number of actual cyber assets communicating with the ESP.

[Attachments \(\)](#)

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this Mitigation Plan:

No additional information to provide.

Appended by NERC

The root cause of the violation was a less than adequate installation/design configuration of the firewalls.

[Attachments \(\)](#)

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

The Mitigation Plan include the following six major milestones:

- 1 Extent of Condition Analysis
- 2 Network Redesign for Control Centers and Substations
- 3 Procure necessary equipment and Establish Baseline Firewall Rules
- 4 Implement Equipment
- 5 Configure Equipment
- 6 Documentation Updates

12/31/2015

Milestone 1: Extent of Condition Analysis

1. Perform an extent of condition analysis to determine the scope.
2. Identify routing patterns/data flows between data centers.

Milestone 2: Network Redesign for Control Centers and Substations

For the substation networks and the Control Center networks, determine the final design and firewall to be utilized and select a vendor.

Milestone 3: Procure necessary equipment and Establish Baseline Firewall Rules

1. Procure necessary equipment for Control Center and Substations.
2. Establish an initial baseline of firewall rules for Control Center and Substations.

Milestone 4: Implement Equipment

1. Deploy procured equipment.
2. Capture network traffic to determine necessary rules.

Milestone 5: Configure Equipment

1. Configure the network equipment.
2. Finalize and implement firewall rules.

Milestone 6: Documentation Updates

1. Complete CIP-007-3 R1 Testing and artifact collection.
2. Verify all necessary network diagrams are updated to reflect changes.
Verify asset lists are updated to remove any old equipment and add new firewall equipment.

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

[REDACTED] to take any additional actions to mitigate this increased risk because we have the following existing mitigating factors in place:

have the following existing mitigating factors in place:

1. Strong authentication into the ESPs (2Factor)
2. Monitoring and alerting of network traffic on a 24x7 period.
3. Cyber assets that access the ESP are equipped with anti-virus softw [REDACTED]
4. Utilization of [REDACTED] through a private VPN for access to Control Centers and Substations.
5. ICCP protocol runs on a private network.

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

As a part of this mitigation plan new network equipment will be implemented. With this new equipment we will be able to implement granular firewall rules rather than more permissive Access Control Lists that are currently being utilized.

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and

• c) Acknowledges:

- I am [REDACTED] of [REDACTED]
- I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
- I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
- I have read and am familiar with the contents of this Mitigation Plan
- [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

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

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

This item was signed by [REDACTED] on 12/17/2015

This item was marked ready for signature by [REDACTED] on 12/15/2015

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for [REDACTED] to verify completion of the Mitigation Plan. [REDACTED] may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

Name of Standard of mitigation violation(s):

Requirement	Tracking Number	NERC Violation ID
R2.	[REDACTED]	[REDACTED]

Date of completion of the Mitigation Plan:

Milestone 1: Extent of Condition Analysis

Milestone Completed (Due: 3/31/2015 and Completed 3/31/2015)

[Attachments \(0\)](#)

1. Perform an extent of condition analysis to determine the scope.
2. Identify routing patterns/data flows between data centers.

Milestone 2: Network Redesign for Control Centers and Substations

Milestone Completed (Due: 5/29/2015 and Completed 5/19/2015)

[Attachments \(0\)](#)

For the substation networks and the Control Center networks, determine the final design and firewall to be utilized and select a vendor.

Milestone 3: Procure necessary equipment and Establish Baseline Firewall Rules

Milestone Completed (Due: 6/30/2015 and Completed 6/29/2015)

[Attachments \(0\)](#)

1. Procure necessary equipment for Control Center and Substations.
2. Establish an initial baseline of firewall rules for Control Center and Substations.

Milestone 4: Implement Equipment

Milestone Completed (Due: 9/4/2015 and Completed 8/31/2015)

[Attachments \(0\)](#)

1. Deploy procured equipment.
2. Capture network traffic to determine necessary rules.

Milestone 5: Configure Equipment

Milestone Completed (Due: 11/30/2015 and Completed 11/30/2015)

[Attachments \(0\)](#)

1. Configure the network equipment.
2. Finalize and implement firewall rules.

Milestone 6: Documentation Updates

Milestone Completed (Due: 12/31/2015 and Completed 12/15/2015)

[Attachments \(0\)](#)

1. Complete CIP-007-3 R1 Testing and artifact collection.
 2. Verify all necessary network diagrams are updated to reflect changes.
- Verify asset lists are updated to remove any old equipment and add new firewall equipment.

Summary of all actions described in Part D of the relevant mitigation plan:

The Mitigation Plan included the following six major milestones:

Description of the information provided to FRCC for their evaluation *

Milestone Completion Evidence provided as follows:

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

CONFIDENTIAL- Non-Public Information

VIA Secure folder & E-MAIL

October 25, 2016

Re: [REDACTED]
Mitigation Plan Verification of Completion
CIP-005-3a R2 [REDACTED]

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED]
[REDACTED] for the referenced violation has been received by the [REDACTED]
[REDACTED] on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
[REDACTED]	CIP-005-3a R2	December 17, 2015

After review for completion, [REDACTED] staff finds that [REDACTED] has completed this
Mitigation Plan. [REDACTED] will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions you may reach [REDACTED]