

## Attachment 3

- 3a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-004-6 R3 submitted February 22, 2018
- 3b. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R3 submitted May 23, 2018
- 3c. The Entity's Verification of Mitigation Plan Completion for CIP-004-6 R3 dated August 28, 2018

This item was signed by [REDACTED] on 2/22/2018

This item was marked ready for signature by [REDACTED] on 2/22/2018

## MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation IDs	Date Submitted	Status	Type	Revision Number
CIP-004-6 R3.	[REDACTED]	[REDACTED]	12/15/2017	Revision Requested	Formal	
CIP-004-6 R3.	[REDACTED]	[REDACTED]	02/14/2018	Revision Requested	Formal	1
CIP-004-6 R3.	[REDACTED]	[REDACTED]	02/22/2018	Region reviewing Mitigation Plan	Formal	2

## SECTION A: COMPLIANCE NOTICES &amp; 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. The final audit report dated [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.



## 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 Human Resources (HR), Information Technology (IT), Corporate Security (CS), [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.

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.

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 required in the future. Additional related forms 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.

[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

[REDACTED] Single Point of Contact (SPOC)



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

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

#### 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:

##### Conduct an Extent of Condition

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

[Attachments \(0\)](#)

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 Completed (Due: 2/28/2018 and Completed 2/28/2018)

[Attachments \(0\)](#)

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.

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

Conducted an Extent of Condition: Identified all Contractors and Service Vendors with CIP access and cross-checked to the PRA evaluations. For all Contractors and/or Service Vendors in which copies of their PRA's were not provided for assessment according to the newly implemented PRA Procedure, their CIP Access was terminated until the PRA contents could be evaluated.

PRA Training Program: Implemented procedure covering the establishment and required documentation for the Personnel Risk Assessment (PRA) Program. The PRA program includes processes and guidelines/instructions for adherence to the required controls and associated control measures established enterprise-wide. In Section 6, titled "Training", is how the initial training will be assigned and tracked. There will annual refresher training required with testing to ensure understanding, (see page 5 of document).

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

Conducted an Extent of Condition: Identified all Contractors and Service Vendors with CIP access and cross-checked to the PRA evaluations. For all Contractors and/or Service Vendors in which copies of their PRA's were not provided for assessment according to the newly implemented PRA Procedure, their CIP Access was terminated until the PRA contents could be evaluated.

PRA Training Program: Implemented procedure covering the establishment and required documentation for the Personnel Risk Assessment (PRA) Program. The PRA program includes processes and guidelines/instructions for adherence to the required controls and associated control measures established enterprise-wide. In Section 6, titled "Training", is how the initial training will be assigned and tracked. There will annual refresher training required with testing to ensure understanding, (see page 5 of document).

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.

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



#### ██████████ Mitigation Plan Verification

To mitigate the violation and prevent its recurrence ██████ agreed to the following:

0. Conduct a preliminary root cause analysis.
1. Develop an enterprise-wide PRA procedure for contractors and vendors.
2. Develop and document controls to ensure Contractor and Service vendor PRA process will be implemented as documented.
3. Develop a training program for Contractor and Service vendor PRAs.
4. Implement updated PRA Procedure.
5. Conduct an Extent of Condition analysis with goal of verifying that 100% of PRAs have been evaluated for Contractors and Service vendors.
6. Add Training Section to PRA Procedure.

As evidence that the Mitigation Plan was completed the following evidence was submitted and reviewed by ██████ staff:

0. CIP004 R3 Meeting Minutes\*.pdf; show evidence the entity conducted multi-departmental meetings to perform a preliminary root cause analysis and develop a mitigation plan based on that analysis.
1. The entity provided two files as evidence of Milestone 1:
  - a. IT-CIP-004-PRO-R3\_Personnel\_Risk\_Assessment-CEll.pdf; PERSONNEL RISK ASSESSMENT PROGRAM, Version 3.0 dated 11/15/2017, All pages, shows updated enterprise-wide PRA procedure for contractors and vendors. Pages 4 and 5, Section 5.2.2 – Contractor Personnel, show steps for business units to follow to verify PRAs for Contractors and Service vendors that have a master contract, and their subcontractors with CIP access. Page 8, Appendix A, shows the form to be used for requesting both the affidavit and a copy of the PRA from Contractors or Service vendors. Pages 9 and 10, Appendix B, show the form to be used for review and documentation of contractor/vendor PRAs. Page 6, Section 7.1 – Retention Period, shows procedural requirement to retain PRA Evaluation & Verification Forms for seven years.
  - b. CIP-004 R3 Contractor PRA Evaluation Form with Instructions.xlsx; Contractor Personnel Risk Assessment (PRA) Evaluation Form, Undated form, shows the EXCEL spreadsheet version of the form used to perform a review of the PRA for Contractors and Service vendors.
2. IT-CIP-004-PRO-R3\_Personnel\_Risk\_Assessment-CEll.pdf; PERSONNEL RISK ASSESSMENT PROGRAM, Version 3.0 dated 11/15/2017, Page 5, Section 5.2.2 – Contractor Personnel, Step 9, requires a PRA Review as a control to ensure Contractor and Service vendor PRA process will be implemented as documented.

3. The entity provided two files as evidence of Milestone 3:
  - a. [REDACTED] CIP-004-TRN-001\_Contractor\_PRA\_Training-CEll.pdf; Contractor Personnel Risk Assessment Training, No revision, Dated 10/30/2017, shows content of training program for contractor and service vendor PRAs.
  - b. PRA Training Evidence 10-30-17 (All Attendees).pdf; Untitled screen shots, Dated 10/30/2017, shows list of attendees for the above-cited training.
4. IT-CIP-004-PRO-R4\_Personnel\_Risk\_Assessment-CEll.pdf; PERSONNEL RISK ASSESSMENT PROGRAM, Version 4.0 dated 11/15/2017, All pages, shows updated enterprise-wide PRA procedure for contractors and vendors, with implementation date of 11/15/2017.
5. The entity provided four files as evidence of Milestone 5:
  - a. CIP-004 R3 Contractor PRA Tracking Matrixes.pdf; CIP 004-6 R3.4 Contractor PRA Tracking Matrixes, Undated, shows a summary of the number of companies contacted, the number of PRAs received, and the number of PRAs reviewed for Contractors or Service vendors with active CIP roles
  - b. PRA Inactivation Report – EAMS 12282017.pdf; “CIP: Training and PRA Report”, Undated report, shows evidence that the “Training and PRA Status” has been set to Inactive for the 13 contractors who no longer have CIP roles.
  - c. [REDACTED] Contractors PRA Revocation Screen Shots.pdf; [REDACTED] Contractors PRA Revocation Screen Shots, Dated 12/28/2017, shows evidence that the seven contractors for whom a PRA evaluation could not be completed, were no longer authorized for any CIP-relevant access as of 12/28/2017.
  - d. [REDACTED] Contractor Revocation and PRA Inactivation Report – EAMS 12282017.pdf; “CIP: Training and PRA Report”, Undated report, shows evidence that the “Training and PRA Status” has been set to Inactive for the seven contractors for whom a PRA evaluation could not be completed.
6. IT-CIP-004-PRO-R5\_Personnel\_Risk\_Assessment-CEll.docx; PERSONNEL RISK ASSESSMENT PROGRAM, Version 5.0 dated 2/28/2018, Page 5, Section 6 – Training, shows that entity has addressed training on the updated enterprise-wide PRA procedure for contractors and vendors. The Training section covers both initial and refresher training and requires testing to confirm understanding of the training materials.

On 8/10/2018 [REDACTED] staff completed their review of the evidence and verified [REDACTED] completed the Mitigation Plan by 2/28/2018.



## Attachment 4

- 4a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-004-6 R4 submitted June 19, 2018
- 4b. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R4 submitted July 20, 2018
- 4c. The Entity's Verification of Mitigation Plan Completion for CIP-004-6 R4 dated August 16, 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 &amp; 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:

According to the Final Audit Report dated [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. [REDACTED]"

[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 Business Unit's 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) The Business Unit 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:

HAS BEEN REDACTED FROM THE PUBLIC VERSION

- 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 Information Technology (IT) "physical" key custodians, their "physical" key custodian roles, and the "physical" key distribution process [REDACTED] re roles are created to manage IT "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] substations 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 [REDACTED] es 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 [REDACTED] and [REDACTED] substations' "physical" key distribution process ensures that "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 custodian role. Completed by October 25, 2017.
- 7: Hold a training session [REDACTED] expectations, responsibilities, and the updated procedure for managing [REDACTED] [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 [REDACTED]. Completed by November 13, 2017.
- 9: Train "physical" key custodians on the responsibilities associated with [REDACTED] CIP access verification process for controlling "physical" keys. Completed by November 13, 2017.
- 10: Revise and implement the IT "physical" key control procedure used to manage IT 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 Business Unit's 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 Business Unit's 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 issuance of the Interim Audit Presentation. An [REDACTED] role did not exist for the Active Directory (AD) group "Domain Admin". As part of an audit data request, an [REDACTED] role was created and assigned to the individuals who were members of the AD group in which a 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 AD domain administrator accounts 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" keys with authorized unescorted [REDACTED] 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 [REDACTED].



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**

The Final Audit Report describes another instance where an individual did not have authorized access to the BES. The individual was found in possession of a "physical" key in their possession. This observance was related to the transfer of a "physical" key during [REDACTED]. An IT Project Manager of the Responsible Entity, realized that the "physical" key to the [REDACTED] was being stored at the [REDACTED] and decided that it would be prudent to have the "physical" key relocated to the [REDACTED]. This would allow the "physical" key to the [REDACTED] to be readily accessible in the event it was needed for access to the PSP, [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 the [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 [REDACTED]. The [REDACTED] who generally travels to the [REDACTED] one day each month, then transported the key to the [REDACTED] and logged it in on August 8, 2016.

Although the [REDACTED] and [REDACTED] did not have authorized unescorted access to the [REDACTED] 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 [REDACTED]. 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 Enterprise-wide Key Management 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 [REDACTED] 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):

Successful completion of this Mitigation Plan [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 detection [REDACTED] 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

[REDACTED] Single Point of Contact (SPOC)



 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 [REDACTED]

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

All Completion Summaries and milestone evidence has been upload to the [REDACTED]

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.

## [REDACTED] Mitigation Plan Verification

To mitigate the violation and prevent its recurrence [REDACTED] agreed to the following:

1. Create a new role in the [REDACTED] for an [REDACTED] within the [REDACTED] Active Directory (AD) domain.
2. Remove "physical" keys from the [REDACTED]. Document by area, the transfer of "physical" keys to the [REDACTED]. Compare [REDACTED] "physical" key control logs to [REDACTED] "physical" key control log to ensure all "physical" keys are logged.
3. Validate Information Technology (IT) "physical" key custodians, their "physical" key custodian roles, and the "physical" key distribution process. Ensure roles are created to manage IT "physical" keys. Validate IT "physical" key custodians have authorized unescorted physical access to the PSPs under their responsibility. Revise "physical" key authorizations and "physical" key distribution process.
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.
5. Document the [REDACTED] process for area access managers to ensure physical keys are only distributed to individuals with authorized access.
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 maintaining and issuing "physical" keys.
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] CIP Access Owner roles.
8. Verify that CIP Access Owner's roles exist for IT, [REDACTED] in [REDACTED] for those responsible for managing "physical" keys. Create CIP Access Owner's roles for "physical" keys in [REDACTED] and report any additional discrepancies identified during verification to the Regional Entities.
9. Train "physical" key custodians on the responsibilities associated with [REDACTED] CIP access verification process for controlling "physical" keys.
10. Revise and implement the IT "physical" key control procedure used to manage IT owned Physical Security Perimeters (PSPs) and High Impact Control Centers.
11. Remediate any discrepancies found in the Extent of Condition performed in milestone 6.
12. Review initial root causes identified during the development of Mitigation Plan, verify that corrective measures have been implemented for root causes and contributing factors.
13. Create an enterprise-wide "physical" key management process for Medium and High Impact Physical Security Perimeters and corresponding process documentation.



14. 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 Business Unit's processes.

As evidence that the Mitigation Plan was completed the following evidence was submitted and reviewed by [REDACTED] staff:

1. Entity provided two files as evidence of this milestone:
  - a. IM-CIP-004-EVD-CIP-004-R4-Mitigation A1-CELL.docx; Mitigation Milestone # 1, Undated screenshot, shows evidence a new role was created in the [REDACTED] for an [REDACTED] on 8/26/2016.
  - b. CIP-004-R4-L13-05\_Evidence-CELL.pdf; DATA REQUEST NARRATIVE RESPONSE, Dated 8/29/2016, Page 7, Table entitled "Users with Shared Access to [REDACTED]" shows a list of the individuals that were granted access to the new [REDACTED] Admin role.
2. Entity provided several files as evidence of this milestone:
  - a. [REDACTED] MEMO.pdf; shows memos sent to [REDACTED] detailing numbers of lock cores and keys to be deployed in their respective Areas.
  - b. [REDACTED] pdf; shows signed acknowledgement from [REDACTED] of their receipt of the lock cores and keys noted in the above-cited memos, with the last being dated 2/9/2017.
  - c. KeyAttestationSU-KA-[REDACTED].pdf; Chain of Custody Agreement, Dated 1/27/2017, shows table detailing numbers of lock cores and keys that were deployed to the respective [REDACTED]
  - d. CIP-004R4 MS2 KeyCount.xlsx; shows spreadsheet used to account for the number of physical keys and their discrete identifier transferred to each [REDACTED]
  - e. Quarterly Access Review\*March 2017.pdf; shows form that was used by each [REDACTED] to verify that those individuals with physical access to BES Cyber Systems have been authorized for such access, with the last being dated 3/27/2017.
3. Entity provided seven files as evidence of this milestone:
  - a. IM-CIP-004\_EVD-KeyControlVisitorAccess\_IMPSPs\_CELL.pdf; Undated meeting invitation, shows that a meeting was scheduled for 12/14/2016 to discuss the key control process for IM Managed PSPs.
  - b. IT-CIP-004-EVD-CIP004\_R4MP\_MS4\_AttestLetterFor121416meeting-CELL.pdf; Attestation Regarding Meeting Attendance, Dated 5/9/2017, documents the list of those in attendance at the aforementioned meeting on December 14, 2016.
  - c. IM-CIP-006-PRO-Key\_Control\_v2.0-CELL.pdf; IM KEY CONTROL PROCEDURE, Version 2.0 dated 9/6/2016, All Pages, shows the IM Key Control Procedure. This Procedure was the main topic of discussion at the aforementioned meeting on December 14, 2016.

- d. IM-CIP-006-PRO-Key\_Control\_DiffBetween2v3-CEII.pdf; IM KEY CONTROL PROCEDURE, Version 3.0 dated 1/31/2017, All Pages, shows redlined version of the changes to the IM Key Control Procedure.
  - e. IT-CIP-004-EVD-Remedy\_Support\_005948104-CEII.pdf; Untitled, Pages 1 and 2 shows ticket for creation of Key Custodian roles, with Date Closed shown as 1/26/2017. Pages 3 and 4 show a Meeting Invite for January 25, 2017, detailing the information needed to create eight new [REDACTED] roles for each of the IT Managed PSPs, including the Key Custodians, Role Owner, Role Name, CIP Access to specific PSPs, and a description of the PSP.
  - f. IM-CIP-004-R4-EvidSumM4\_New [REDACTED] KeyCustRoles-CEII.xlsx; Undated Excel workbook, AccessVerify tab, shows the EXCEL workbook that was generated from [REDACTED]. In the "AccessVerify" spreadsheet is a list of the Key Custodians that were assigned the new roles. After confirming that the new Key Custodian roles were created, an IT CIP office representative performed a manual validation to confirm that each of the Key Custodians have authorized unescorted physical access to the assigned site(s).
  - g. IM-CIP-004-R4-ExcelValidationKeyCustodiansIM-CEII.pdf; System output dated 2/27/2017, shows [REDACTED]-generated list that was used to validate the Key Custodians who have authorized unescorted physical access to IT managed PSPs. The report also shows all the unescorted physical access roles assigned to each Key Custodian.
4. Entity provided several files as evidence of this milestone:
- a. IT-CIP-004-EVD-Cyber\_Physical\_Roles\_20170419-CEII.pdf; System output dated 4/19/2017, shows an [REDACTED]-generated report listing roles that had both physical and electronic access to BES Cyber Assets.
  - b. IT-CIP-004-EVD-Roles\_PIT\_20170501-CEII.pdf; System output dated 5/1/2017, shows an [REDACTED] generated report listing CIP-related roles.
  - c. [REDACTED] CIP-004-EVD-Roles\_PIT\_20170818-CEII.pdf; System output dated 8/18/2017, shows evidence that no CIP physical access role is still also granting electronic access to Cyber Assets.
  - d. \*-CIP-004-EVD-Physical\_Access\_Matrix\_201708\*-CEII.pdf; Undated system output, shows unescorted physical access matrices by business unit. These reports list all CIP unescorted physical access roles and define which PSP the [REDACTED] role is authorizing access. No role was found to grant both physical and cyber access.
5. Entity provided several files as evidence of this milestone:
- a. 15\_06\_02\*.docx; CIP SUBSTATION PHYSICAL SECURITY PLAN, show a series of updates to the physical security plan used by [REDACTED] with the last update showing an effective date of 8/29/2017. Section 6.1 (Key Control – Overview) includes the newly required process step for [REDACTED] to verify that a Substation key requestor has authorized unescorted physical access prior to issuing a physical key.
  - b. CIP-006 Procedure Update B to C Training Invite.pdf; Undated meeting invitation, shows that a meeting was scheduled for 1/30/2017 to train [REDACTED] responsible for the protection and distribution of physical keys in regard to the updated "physical" key distribution procedure.



6. Entity provided several files as evidence of this milestone:
- a. [REDACTED] CIP-006-[REDACTED]-001-Key\_Control\_and\_Inventory\_091316-CELL.pdf; Key Control and Inventory Template Form, Dated 9/13/2016, shows the file used to record the verification performed at [REDACTED] facility, showing the reviewer accounted for all physical keys.
  - b. [REDACTED] CIP-006-[REDACTED]-001-Key\_Control\_and\_Inventory\_121216-CELL.pdf; Key Control and Inventory Template Form, Dated 12/12/2016, shows the file used to record the verification performed at [REDACTED] facility, showing the reviewer accounted for all physical keys.
  - c. [REDACTED] CIP-004 [REDACTED] Role [REDACTED] LockboxKey-EMP-CELL.pdf; Active Access Report for Role Owners, [REDACTED] system output dated 5/22/2017, shows evidence the key custodians (Primary and Backup [REDACTED]) are assigned a CIP role.
  - d. [REDACTED] CIP-004 [REDACTED] Role PWC LockboxKey-EMP-CELL.pdf; Active Access Report for Role Owners, [REDACTED] system output dated 5/22/2017, shows evidence that individuals with access to the lockbox where keys are stored (Maintenance Leaders and [REDACTED]) are assigned a CIP role.
  - e. [REDACTED] CIP-006-INS-002-Key\_Control\_V2.0-CELL.pdf; Key Control, Version 2.0 dated 6/6/2017, Pages 2 and 3, Section 5.3 - Key Control and Inventory (R1.1 & R1.2), shows evidence the [REDACTED] Key Control Standard was enhanced to ensure that individuals are aware of the required authorization/access management role required to both manage and request access to the physical keys. This was done by adding the following statements: "Cabinet Access Keys require the [REDACTED] Role: [REDACTED] - XXX - PHYSICAL-EMP", "Lockbox Keys require the [REDACTED] Role: [REDACTED] - XXX LOCKBOX KEY-EMP", and "Override Keys require the [REDACTED] Role: [REDACTED] - XXX - PHYSICAL-EMP".
  - f. [REDACTED] CIP-006-EVD-Key\_Control\_Notifications-CELL.pdf; Emails to [REDACTED] - [REDACTED], shows acknowledgements from [REDACTED] and delegates that they have read the updated Key Control Standard.
  - g. [REDACTED].pdf; show signed acknowledgement from [REDACTED] of their receipt of lock cores and keys, with the last being dated 2/9/2017.
  - h. [REDACTED] Quarterly Access Review\*March 2017.pdf; show evidence that a [REDACTED] representative for each Area reviewed the "Key Control Register and Inventory Form C6-02", and compared it against the Key Attestation (see [REDACTED] pdf citation above). The result was that all physical keys currently assigned to authorized individuals have been accounted for; however, there were keys not in circulation that were not accounted for. As a result, Medium Impact Substations are to be re-cored and new keys issued, replacing all existing keys. This activity is documented as part of milestone 11.
  - i. 15\_06\_02\_G-CIP Substation Physical Security Plan.pdf; CIP SUBSTATION PHYSICAL SECURITY PLAN, Revision G dated 10/13/2017, Page 2, Section 3 – Roles and Responsibilities, shows evidence the [REDACTED] CIP Substation Physical Security Plan was enhanced to ensure that individuals are aware of the required authorization/access management role required to both manage and request access to the physical keys. This was done by adding the following statement: "[REDACTED] SUBSTATION AREA MANAGER - <area name>".

j. [REDACTED] Key Management Procedures Update Notification.pdf; Email to [REDACTED] and delegates, Dated 10/13/2017, shows notification sent to Key Custodians regarding the above-cited change to the CIP Substation Physical Security Plan.

7. Entity provided seven files as evidence of this milestone:

a. [REDACTED] CIP-004-EVD-Role\_Owner\_Training 20170301-CELL.pptx; CIP-004-6 Role Life Cycle Management and Role Owner Responsibilities, Dated 3/2017, shows training presentation for all [REDACTED] and Delegates regarding on the expectations, responsibilities, and the revised access management procedures for "physical" keys.

b. [REDACTED] CIP-004\_EVD-Role\_Owners\_Attendees-CELL.xlsx; Role Owners Training Attendance (3/22/2017 & 4/5/2017), shows evidence entity tracked attendance at two training sessions, and tracked email confirmation of understanding from individuals who were unable to attend in person.

c. IT-CIP-004-EVD-IT\_RO\_Training1-CELL.pdf; Emails from [REDACTED], shows evidence of confirmation of understanding from 22 individuals who were unable to attend the aforementioned training in person.

d. IT-CIP-004-EVD-IT\_RO\_Training2-CELL.pdf; Emails to [REDACTED], shows evidence of confirmation of understanding from 5 individuals who were unable to attend the aforementioned training in person.

e. [REDACTED] CIP-004-EVD-RO\_Training-CELL.pdf; No revision, Undated; shows evidence of confirmation of understanding from 12 individuals who were unable to attend the aforementioned training in person.

f. CIP-004-6\_R4\_MS\_7\_[REDACTED]\_Role\_Owner\_Training\_CELL.pdf; emails to [REDACTED], shows evidence of confirmation of understanding from 10 individuals who were unable to attend the aforementioned training in person.

g. [REDACTED] CIP-004\_EVD-RO\_Training\_Example-CELL.pdf; Email from [REDACTED], Dated 8/28/2017, shows an entity-selected example of the training presentation being emailed to a new Role Owner.

8. Entity provided five files as evidence of this milestone:

a. [REDACTED] CIP-004-EVD-Key\_Custodian\_Roles-CELL.pdf; Email from [REDACTED], Dated 5/12/2017, shows list of [REDACTED] Role Names assigned to the Key Custodians for [REDACTED].

b. [REDACTED] CIP-004-EVD-Key\_Custodian\_Roles-CELL.pdf; Email from [REDACTED], Dated 5/11/2017, shows list of [REDACTED] Role Names assigned to the Key Custodians for [REDACTED].

c. IM-CIP-004-R4-ExcelValidationKeyCustodiansIM-CELL.pdf; System output dated 2/27/2017, lists authorized individuals who can manage physical keys, their key management role(s), and their unescorted access role(s).

d. [REDACTED] CIP-004-EVD-Key\_Custodian\_Active\_Users\_20170601-CELL.pdf; System output dated 6/1/2017, shows the [REDACTED] report that was generated to validate that the roles exist and are assigned to the appropriate individuals in [REDACTED].

e. [REDACTED] CIP-004-EVD-Key\_Custodian\_Active\_Users\_20170601-CELL.pdf; System output dated 6/1/2017, shows the [REDACTED] report that was generated to validate that the roles exist and are assigned to the appropriate individuals in [REDACTED].



9. Entity provided several files as evidence of this milestone:

- a. [REDACTED] CIP-004-EVD-Key\_Cust\_Training\_FINAL-CELL.pptx; NERC Critical Infrastructure Protection (CIP) Key Custodian Access Management Training, Dated 3/1/2017, shows training presentation designed to educate Key Custodians on their key roles and responsibilities.
- b. [REDACTED] CIP-004-EVD-Key\_Custodian-Training\_Roster-CELL.xlsx; NERC Critical Infrastructure Protection (CIP) Key Custodian Access Management Training, shows evidence entity tracked attendance at two training sessions, and tracked email confirmation of understanding from individuals who were unable to attend in person.
- c. [REDACTED] CIP-004-EVD-Key\_Custodian\_Training\_Multiple-CELL.pdf; Emails to [REDACTED], shows evidence of confirmation of understanding from 6 [REDACTED] individuals who were unable to attend the aforementioned training in person.
- d. [REDACTED] CIP-004-EVD-Key\_Custodian\_Training\_[REDACTED]-CELL.pdf; email from Sr [REDACTED] Maintenance Specialist to [REDACTED] Sr. Compliance Specialist, Dated 7/31/2017, shows evidence of confirmation of understanding from the sole Power [REDACTED] individual who was unable to attend the aforementioned training in person.

10. Entity provided three files as evidence of this milestone:

- a. IM-CIP-006-PRO-Key\_Control\_REDLINE\_v3.0-CELL.pdf; IM KEY CONTROL PROCEDURE, Version 3.0 dated 1/31/2017, Pages 1-3, Section 5 – Procedure / Instructions, shows updates made to key control procedure used to manage IT-owned PSPs and High Impact Control Centers. Pages 8 and 9, Appendices C and D, show the list of approved Key Custodians, along with the list of roles for unescorted physical access.
- b. IM-CIP-006-PRO-Key\_Control\_REDLINE\_v3.1-CELL.pdf; IT KEY CONTROL PROCEDURE, Version 3.1 dated 11/14/2017, All pages, shows further enhancements to the above-cited procedure including: additional unescorted access roles that did not originally exist, the list of key custodian roles, a process for lost and found keys, and re-coring.
- c. IT-CIP-006-EVD-Email\_Notification.pdf; Email from [REDACTED] to key custodians, dated 11/14/2017, shows evidence notification was sent to Key Custodians of IT-managed PSPs, regarding the approval and implementation of the updated Key Control Procedure.

11. Entity provided several files as evidence of this milestone:

- a. TSO\_Core\_Key\_Replacement\_Email.pdf; Email from [REDACTED] to [REDACTED] Dated 6/27/2017, shows evidence that [REDACTED] were notified of required Core/Key replacement activity, and the deadline associated with completing the core replacements.
- b. Substation\_Re-core\_Evidence\_Attestation\*.pdf; show evidence that the entity tracked completion of the re-coring of relay vault doors, the last of which occurred on 7/17/2017.
- c. Substation\_Re-Core\_Evidence\_C6-02\*.pdf; Key Control Register and Inventory Form - C6-02, show completed forms that were created for the new keys at medium substations. The forms also list the authorized individuals who have possession of specific keys, as well as the keys that are kept in a locked storage location. The last of these forms were completed on 8/3/2017.

12. [REDACTED] CIP-004-EVD-Root\_Causes\_Analysis\_Validation-CEll.pdf; Untitled table, shows entity statement that "On November 17, 2017, representatives from each business unit validated all actions that were performed to correct the key distribution issues the table below was finalized based on the input in the meeting." The statement also reports that "No additional causes have been identified."

13. Entity provided three files as evidence of this milestone:

a. CS-CIP-006-PRO-PSPKeyMgmt\_CEll.docx; ENTERPRISE KEY MANAGEMENT PROCEDURE, Version 1 dated 3/5/2018, shows newly developed Enterprise Key Management Procedure owned by Corporate Security.

b. CS-CIP-006-TMP-PSPKeyInventoryReview\_CEll.docx; ENTERPRISE KEY INVENTORY REVIEW TEMPLATE – CIP PHYSICAL SECURITY PERIMETERS, Undated blank form, shows form that will be used to conduct quarterly reviews of the physical keys for each Medium and High Impact PSP.

c. CS-CIP-006-TMP-PSPKeyRegister\_CEll.docx; ENTERPRISE KEY REGISTER TEMPLATE – CIP PHYSICAL SECURITY PERIMETERS, Undated blank form, shows form that will be used at each of the PSPs to track when physical keys are "checked-out" and "checked-in" to individuals with authorized unescorted access to the PSP.

14. Entity provided four files as evidence of this milestone:

a. [REDACTED] CIP-004-EVD-CoverSheet\_MS14\_CEll.docx; Untitled, Dated 2/9/2018, shows an SME's summary of the training activities performed to support the implementation of the new Enterprise Key Management Procedure.

b. [REDACTED] CIP-004-EVD-PSP\_Key\_Mgmt\_Training\_Cal\_Invite\_CEll.pdf; Undated meeting invitation, shows that a meeting was scheduled for 1/31/2018 to provide Enterprise Key Management Procedure training.

c. [REDACTED] CIP-004-EVD-PSP\_Key\_Mgmt\_Training\_PPDeck\_CEll.pdf; Key Management Training Module, Undated presentation, shows the "Key Management Training Module" PowerPoint presentation that was used to conduct the training performed on Wednesday, January 31, 2018.

d. [REDACTED] CIP-004-EVD-R4\_MS14\_Training\_Emails\_Confirms\_CEll.pdf; Emails to [REDACTED], shows email confirmations of review and understanding of the "Key Management Training Module" presentation from those individuals that did not attend the live training session. The last of these confirmations were dated 2/9/2018.

On 8/16/2018 [REDACTED] staff completed their review of the evidence and verified [REDACTED] completed the Mitigation Plan by 2/9/2018.



## Attachment 5

- 5a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-005-5 R1 submitted May 30, 2018
- 5b. The Entity's Certification of Mitigation Plan Completion for CIP-005-5 R1 submitted September 18, 2018
- 5c. The Entity's Verification of Mitigation Plan Completion for CIP-005-5 R1 dated May 9, 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-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:

In the final audit report dated [REDACTED] the auditors found 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:

The Responsible Entity has no relevant information.

##### [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, or to Confirm 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: 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 . 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,  
ed  
h  
by

4: Perform an Extent of Condition to develop a complete inventory list of existing documentation. The inventory of documentation will include policies, procedures, work  
MES  
by

5: Perform an Extent of Condition Analysis of all the High Impact BCS EAPs, which will include those used in the performance of the function, 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 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, with status and completion date for each Milestone or Activity identified above. 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 a [REDACTED] network protections, the risk of unauthorized access by an external party through ICMP at the Medium Impact BES Cyber System is very low.

[REDACTED]

[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]

[REDACTED]

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



EAPs requires a thorough analysis and review before the more restrictive rules can safely be implemented without impacting system operations and the reliability of the High and Medium Impact BES Cyber Assets. Additionally, the implementation of the new firewall rules must be properly coordinated with scheduled maintenance outages to avoid unplanned system outages.

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

#### [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

[REDACTED] Single Point of Contact (SPOC)

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 [REDACTED] as agreed to during conference call with enforcement on September 17, 2018.

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

As of the completion of Milestone 15, all deficiencies have been addressed and the evidence will be uploaded to the [REDACTED] as agreed to during conference call



with enforcement on September 17, 2018.

**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.

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 Information Technology (IT) and [REDACTED] 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, which will include those used in the performance of the [REDACTED] function, 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 [REDACTED] 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.

████████████████████  
████████████████████ staff completed their review of the evidence and verified ██████████ completed the Mitigation Plan by 9/18/2018.

## Attachment 6

- 6a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-006-3c R1 submitted May 23, 2018
- 6b. The Entity's Certification of Mitigation Plan Completion for CIP-006-3c R1 submitted June 11, 2018
- 6c. The Entity's Verification of Mitigation Plan Completion for CIP-006-3c R1 dated August 17, 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 &amp; 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:

In the Final Audit Report dated [REDACTED] it states the Responsible Entity, "did not properly maintain complete visitor access control logs for [REDACTED] PSP. As a result, [Responsible Entity] was not in compliance with the CIP Reliability Standard CIP-006-6 Requirement R2. [REDACTED]"

"[Responsible Entity] maintained visitor access logs that documented access into its PSPs. The audit team reviewed the access logs at [REDACTED] P. 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:

To put this possible violation ("[REDACTED]") into proper perspective, it is important to note that the Physical Security Perimeters (PSPs) at the [REDACTED] located 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] at [REDACTED] these visitors were on the floor but not necessarily entering the PSPs. In any event, the functional obligations of the Responsible Entity's [REDACTED] 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 [REDACTED] 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 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: 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

[REDACTED] Single Point of Contact (SPOC)

 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 [REDACTED]

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

Completion Summaries and all supporting evidence were uploaded to the [REDACTED]

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.



[REDACTED] Mitigation Plan Verification

[REDACTED] Mitigation Plan Validation

[REDACTED]  
To mitigate the violation and prevent its recurrence [REDACTED] agreed to the following:

0. Preliminary assessment of root causes.
1. Evaluate the process for reviewing visitor access logs and identify enhancements that need to be incorporated.
2. Review the process that is utilized by those who have authorized unescorted physical access; and, identify enhancements that need to be incorporated.
3. Perform an Extent of Condition.
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.
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.
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.

As evidence that the Mitigation Plan was completed the following evidence was submitted and reviewed by [REDACTED] staff:

0. CS-CIP-006-EVD\_R2MitPlan\_MS0\_Attestation\_CELL.pdf; Letter from [REDACTED], [REDACTED], Dated 5/15/2018, shows letter of attestation stating that a preliminary assessment of root causes was completed by 12/31/2016. It further states that two primary causes were discovered: the quarterly access log review process was inadequate, and individuals with authorized unescorted physical access were inadequately trained.
1. Entity provided two files as evidence of this milestone:
  - a. CS-CIP-006-EVD\_R2MS1\_MeetMins\_WorkSess\_CELL.pdf; Email from [REDACTED], [REDACTED], Dated 2/21/2017, shows communication summarizing a meeting to review the process each Business Unit used for escorted access within a Physical Security Perimeter (PSP), including how each individual was documented in a visitor log.
  - b. 15\_06\_02\_C-CIP Substation Physical Security Plan.pdf; CIP SUBSTATION PHYSICAL SECURITY PLAN, Revision C dated 10/28/2016, Pages 6 and 7, Section 7 – Visitor Access Log Review, shows

instructions on how to perform quarterly reviews of visitor logs in the [REDACTED] business unit. It was noted that such instructions should be added to other business units' plans as well.

2. Entity provided two files as evidence of this milestone:

- a. CS-CIP-006-EVD\_R2MS2\_Email\_2\_28\_[REDACTED]AddEnh\_CEII.pdf; Email chain, Dated 2/28/2017, describes planned enhancements to the visitor logging process, as identified during review of said process.
- b. C6-01-SubstationVisitorAccessLog\_CEII.xlsx; Substation Visitor Log, No revision, Undated, shows spreadsheet visitor sign-in form that will be used at substations, as well as at other PSPs, as a backup log form when the electronic system "[REDACTED]" is out-of-service.

3. Entity provided several files as evidence of this milestone:

- a. ALL-CIP006-EVD-R2MS3 MPSumOfDiscrep\_CEII.xlsx; Undated spreadsheet, summarizes the number of discrepancies discovered during the Extent of Condition analysis, broken out by business unit and by location.
- b. CIP006-R2M3\_LogReview\_\*.pdf; show attestations collected from each employee responsible for performing the review of each PSP visitor access log, listing the discrepancies discovered during these reviews. The last of these are dated 4/24/2017.

4. Entity provided two files as evidence of this milestone:

- a. CS-CIP-006-PRO-PSPVisitorMgmt\_CEII.docx; ENTERPRISE VISITOR MANAGEMENT PROCEDURE, Version 1.0 dated 1/1/2018, Pages 1 – 5, Sections 5.1 – 5.4, shows newly developed enterprise-wide visitor management procedure integrating the enhancements identified during milestones 1 and 2.
- b. CS-CIP-006-TMP-VisitorAccessLogs\_Reviews\_CEII.xlsx; [REDACTED] Visitor Access, No revision, Undated, shows workbook that will be used enterprise-wide for documenting visitor access to PSPs, and performing the quarterly reviews. The spreadsheet titled "Cover Sheet" is where the 'Site Name' will be entered for the PSP access point. The "Visitor Log Template" spreadsheet is a standardized log-in sheet. It also contains the warning statement, "NOTE: Failure to complete ALL fields is a violation of the Reliability Standard and may result in a penalty and/or result in disciplinary action". The "Visitor Log Review Template" is the spreadsheet that must be completed during performance of the quarterly review of the visitor log; and, a spreadsheet titled, "Visitor Log Review Sample" which provides an example of the how the fields in the spreadsheet should be populated when a log review is performed.

5. CIP006-EVD\_R2M5\_\*.pdf; show attestations intended to close out incomplete log entries where possible.

6. Entity provided two files as evidence of this milestone:

- a. CS-CIP006-EVD-R2MS6\_VisitorMgmtTrng\_CEII.pdf; CIP-006 R2 Mitigation Plan – Milestone 6 Execution Evidence, Dated 12/15/2017, shows explanation of the activities completed to identify all individuals who would need to be trained on the new Enterprise-wide Visitor Management Procedure. This file also explains the activities completed to develop the training deck. All individuals who



completed the training are listed, and the steps that were taken for people who failed to complete the training are described.

b. [REDACTED] CIP006-EVD-PSP\_VisitorMgmtTrng\_CELL.pdf; Visitor Control Training Module, No revision, Undated, shows content of training material regarding the new enterprise-wide Visitor Management Procedure.

On 8/17/2018 [REDACTED] staff completed their review of the evidence and verified [REDACTED] completed the Mitigation Plan by 12/15/2017.

Note: While the newly developed procedure cited for milestone 4 shows an effective date of 1/1/2018, [REDACTED] noted the training that completed the return to compliance was conducted by 12/15/2017.

## Attachment 7

- 7a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-006-6 R1 submitted February 22, 2018
- 7b. The Entity's Certification of Mitigation Plan Completion for CIP-006-6 R1 submitted May 18, 2018
- 7c. The Entity's Verification of Mitigation Plan Completion for CIP-006-6 R1 dated August 17, 2018



This item was signed by [REDACTED] on 2/22/2018

This item was marked ready for signature by [REDACTED] on 2/22/2018

## MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation IDs	Date Submitted	Status	Type	Revision Number
CIP-006-6 R1.	[REDACTED]	[REDACTED]	01/02/2018	Revision Requested	Formal	
CIP-006-6 R1.	[REDACTED]	[REDACTED]	02/22/2018	Region reviewing Mitigation Plan	Formal	1

## SECTION A: COMPLIANCE NOTICES &amp; 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:

In the final audit report dated [REDACTED] it states the Responsible Entity, "did not implement two or more different physical access controls to allow unescorted physical access into its Local [REDACTED] 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]

## Attachments ( )

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

The [REDACTED] 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 [REDACTED] in the important security objective of controlling access to [REDACTED], 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.

## 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: Update the Physical Security Perimeter (PSP) at the [REDACTED] 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 [REDACTED] will no longer monitor the foyer as a PSP. Completed by October 19, 2016.
- 2: Revise/update the Physical Security Perimeter drawing for the [REDACTED] 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 [REDACTED] 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, [REDACTED] that reduced the likelihood of misuse or undetected un [REDACTED] 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] 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))

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

- 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

[REDACTED] Single Point of Contact (SPOC)

 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 with supporting evidence was uploaded to [REDACTED] [REDACTED] on March 14, 2018.

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

The Milestone Completion Summaries with supporting evidence was uploaded to [REDACTED] [REDACTED] on March 14, 2018.

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.



[REDACTED] Mitigation Plan Verification

[REDACTED] Mitigation Plan Validation

[REDACTED]

To mitigate the violation and prevent its recurrence [REDACTED] agreed to the following:

1. Update the Physical Security Perimeter (PSP) at the [REDACTED] site to remove the foyer area.
2. Revise/update the PSP drawing for the [REDACTED] to properly illustrate the foyer area and its authentication controls.
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.
4. Correct any egress only doors that allow entry into a High Impact PSP found during walkdown in Milestone 3.
5. Review Enterprise-wide Physical Security Plan to determine whether design expectations related to egress only doors are described within the Plan.
6. Schedule and administer a training session for physical security design Personnel on the design expectations required for egress only doors.
7. Revise [REDACTED] 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.
8. Train [REDACTED] on the Updated [REDACTED] Procedure.

As evidence that the Mitigation Plan was completed the following evidence was submitted and reviewed by [REDACTED] staff:

1. Entity submitted several files as evidence of this milestone:
  - a. CS-CIP-006-EVD\_PSDrawing\_[REDACTED] Before\_CELL.pdf; Page 1, shows the layout for Access Control Devices at the [REDACTED] prior to PSP change. Pages 2 – 4 show report generated from the Physical Access Control System (PACS), listing controls in place at [REDACTED] prior to PSP change; entity has highlighted programming that was removed as part of the PSP update.

- b. CS-CIP-006-EVD-ICD20603\_CELL.pdf; Page 8, shows a change ticket in the Change Management system was submitted by the Manager of Critical Infrastructure and Compliance in the [REDACTED] Business Unit to initiate the removal of the access card reader for the small foyer area from the [REDACTED] Page 1, Schedule Dates section, shows work was completed on 10/20/2016.
- c. CS-CIP-006-EVD-BadgeAlarmHistory\_[REDACTED]10\_19\_CELL.pdf; PACS output, shows badge history before and after foyer area was removed from the [REDACTED]
- d. CS-CIP-006-EVD-PACS\_[REDACTED]After\_CELL.pdf; Undated PACS output, shows the controls in place after removing the exterior door from PACS.
2. CS-CIP-006-EVD\_PSDrawing\_[REDACTED]After\_CELL.pdf; PSP diagram dated 12/7/2016, Page 2, shows evidence the PSP drawing for the [REDACTED] has been updated to properly illustrate the foyer area and its authentication controls. The foyer is no longer depicted as being a part of a PSP, and the diagram shows "Protected Cabling" traversing the foyer, as it sits between two separate PSP segments. Page 8 provides description of the specific changes made in the PACS.
3. CS-CIP-006-EVD-R1M3\*.vsd, show PSP diagrams and photographs taken on or before 3/24/2017, demonstrating that walk-downs confirmed there were no mechanisms in place to allow for entry into high impact PSPs from any egress-only doors.
4. CIP-006 R1 MS04 [REDACTED] Completion Summary.docx; Summary of Completed Milestone Activity, Dated 4/28/2017, explains that no action was required for milestone 4 based on the results of milestone 3. For milestone 4, the entity agreed to correct any egress-only doors that allow entry into a High Impact PSP, if found during walkdown in Milestone 3. As documented for milestone 3, no such doors were found, so no such corrections were necessary.
5. Entity submitted two files as evidence of this milestone:
  - a. CS-CIP-006-EVD-EgressReviewTrngSess\_MtgMin\_CELL.pdf; CIP006 R1 Mitigation Plan Egress Training Milestone, Dated 5/10/2017, shows agenda and notes from the meeting to review the Enterprise Physical Security Plan specifically covering the design expectations for egress only doors.
  - b. CS-CIP-006-PLN-PhysicalSecurityPlan(002-08)\_20170401\_CELL.pdf; Enterprise Physical Security Plan CIP 006-6, Revision 2 dated 4/1/2017, Pages 7 and 8, Sections 10.1.2 and 10.1.5, show evidence the existing enterprise-wide Physical Security Plan describes design expectations related to egress-only doors.
6. Entity submitted two files as evidence of this milestone:
  - a. CS-CIP-006-EVD-EgressPSPOpeningsTraining\_CELL.pdf; Egress PSP Openings – Training, Dated 5/10/2017, shows evidence the training for this milestone simply covered Sections 10.1.2 and 10.1.5 of the Enterprise-wide Physical Security Plan.
  - b. CS-CIP-006-EVD-EgressReviewTrngSess\_MtgMin\_CELL.pdf; CIP006 R1 Mitigation Plan Egress Training Milestone, Dated 5/10/2017, shows agenda and notes from the meeting to train on the Enterprise Physical Security Plan specifically covering the design expectations for egress only doors.
7. CS-CIP-006-EVD\_FSRs\_COMPARE\_BTW\_rev4\_rev8\_CELL.pdf; [REDACTED], Revision 8 dated 6/29/2017, Pages 5 – 8, [REDACTED] Execution section, shows evidence the [REDACTED]



██████████ Procedure was revised to include language which requires physical security drawings to be reviewed as part of any physical security facility review; and, to discuss with the business unit any changes or modifications that may have been made prior to the walk-down, and to document any exceptions during the walk-down.

8. Entity submitted two files as evidence of this milestone:

a. CS-CIP-006-EVD-R1MS8\_██████████ TrainingSignInSheet\_CELL.pdf; ██████████ Training – Sign In Sheet, Dated 10/10/2017, shows signatures of the ██████████ who attended training required by this milestone.

b. CS-CIP-006-EVD-R1MS8\_██████████ TrainingDeck\_CELL.pdf; ██████████ Training, Dated 10/10/2017, shows contents of the training materials required by this milestone.

On 8/17/2018 ██████████ staff completed their review of the evidence and verified ██████████ completed the Mitigation Plan by 10/10/2017.

## Attachment 8

- 8a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-3a R2 submitted June 4, 2018
- 8b. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R2 submitted August 17, 2018
- 8c. The Entity's Verification of Mitigation Plan Completion for CIP-007-3a R2 dated May 9, 2019



This item was signed by [REDACTED] on 6/4/2018

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]	06/04/2018	Region reviewing Mitigation Plan	Formal	

## SECTION A: COMPLIANCE NOTICES &amp; 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:

The Final Audit Report dated [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).

[REDACTED]

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), including those involved with the performance of the [REDACTED] function, are working collaboratively on the milestone activities in this Mitigation Plan. Personnel from Information Technology (IT), [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 the execution of the program. The effort in building and documenting 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 \(\)](#)

#### 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 Information Technology (IT), [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 for IT, [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 ports and services [REDACTED] in the inventory list created in milestone 2 for IT, [REDACTED] BUs. 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 for IT, [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 ports and services currently in effect for IT, [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]  
[REDACTED] EOC 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:



Milestone Pending (Due: 8/17/2018)

HAS BEEN REDACTED FROM THIS PUBLIC VERSION

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.

## 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 that is responsive to the possible violation (PV) in the Final Audit Report; and, the Mitigation Plan will be [REDACTED] erim 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) while the Responsible Entity executes this Mitigation Plan.

To begin, the goal of CIP-007-6 Requirement R1 is to minimize the attack surface of BES Cyber Systems through disabling or limiting access [REDACTED] ry network accessible logical ports and services and physical input/output ports. This important security requirement is nonetheless location and device specific. For example, the [REDACTED] system cited in the Final Audit Report was a Medium Impact BES Cyber System located at a [REDACTED] within a Physical Security Perimeter (PSP), and an Electronic Security Perimeter (ESP). Likewise, the [REDACTED] is located inside a Control Center that is within a PSI [REDACTED]. To assess what, if any, BES reliability risk may be posed by inadequate ports and services documentation for these BES Cyber Assets, one must factor into the equation that the Responsible Entity had, and continues to have in-place multi-layered protections designed to protect against unauthorized physical and electronic access to all of its corporate networks and Cyber Assets that the company views as critical to operations. This defense-in-depth posture is even more pronounced for the High and Medium Impact BES Cyber Systems of the type referenced in the PV finding, for which physical access is protected in accordance with CIP-006-6, and remote electronic access is protected in accordance with CIP-005-5 Requirement R2. Details on the Responsible Entity's defense-in-depth posture for physical access is set forth in the co [REDACTED] ical Security Plan for CIP-006-6, and is addressed in the Interim Risk Statements for the CIP-006-6 Requirements R1 and R2 Mitigation Plans. (For a detailed description of the Responsible Entity's defense-in-depth posture for electronic access, please reference the Interim Risk Statement provided in [REDACTED] Requirement R1 Mitigation Plan, and the Responsible Entity's CIP-005-5 Requirement R2 procedure for Interactive Remote Access Management attached.)

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.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The risk to the reliability of the BES remains minimal during the execution phase of this Mitigation Plan. While the Responsible Entity found issues within its program documentation during the Extent of Condition analysis completed October 25, 2017, (see Milestone 6); the lack of adequate documentation supporting enabled ports and services for Cyber Assets will be resolved for all devices once the Mitigation Plan is complete. In the meantime, the Responsible Entity's BES Cyber Systems will continue to be protected by the strong physical and electronic security defense-in-depth posture and controls already implemented for CIP-006-6 Requirements R1 and R2, and CIP-005-5 Requirement R2. Collectively, these protections greatly reduce any putative risk to the reliability of the BES that may be posed by documentation issues.

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 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

[REDACTED] Single Point of Contact (SPOC)



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.

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 all supporting evidence will be uploaded to the [REDACTED]

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

Completion Summary and all supporting evidence will be uploaded to the [REDACTED]

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.

## [REDACTED] Mitigation Plan Verification

## [REDACTED] Mitigation Plan Validation

1: Create an inventory list of policies, standards, procedures, and work instruction documentation for ports and services currently in effect for Information Technology (IT), [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 for IT, [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 ports and services implementation evidence templates in the inventory list created in milestone 2 for IT, [REDACTED] BUs. 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 for IT, [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 ports and services currently in effect for IT, [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.

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. 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 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 – CELL" 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.

[REDACTED]

[REDACTED] staff completed their review of the evidence and verified [REDACTED] completed the Mitigation Plan by 8/17/2018.



## Attachment 9

- 9a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-3a R3 submitted June 7, 2018
- 9b. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R3 submitted February 28, 2019
- 9c. The Entity's Verification of Mitigation Plan Completion for CIP-007-3a R3 dated May 9, 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 &amp; 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:

In the final audit report dated [REDACTED] it stated the Responsible 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, [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), including those involved with the performance of the [REDACTED] function, are working collaboratively on the milestone activities in this Mitigation Plan. Personnel from Information Technology (IT), [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, for this 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: Create an inventory list of policies, standards, procedures, and work instruction documentation for security patch management currently in effect for Information Technology (IT), [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 for IT, [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 for IT, [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 for IT, [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 for IT, [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 [REDACTED]. 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.



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) 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.

## 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.

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

[REDACTED] Single Point of Contact (SPOC)



This item was signed by [REDACTED] on 2/28/2019

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
R3.	[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 together and uploaded to the [REDACTED]

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

Evidence for all milestones will be packaged together and uploaded to the [REDACTED]

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.

██████████ Mitigation Plan Verification

1: Create an inventory list of policies, standards, procedures, and work instruction documentation for security patch management currently in effect for Information Technology (IT), ██████████

██████████ 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 for IT, ██████████ 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 for IT, ██████████ 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 for IT, ██████████ 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 for IT, ██████████ 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 [REDACTED]. 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.



[REDACTED]

[REDACTED] staff completed their review of the evidence and verified [REDACTED] completed the Mitigation Plan by 8/17/2018.

## Attachment 10

- 10a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-6 R3 submitted May 30, 2018
- 10b. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R3 submitted August 17, 2018
- 10c. The Entity's Verification of Mitigation Plan Completion for CIP-007-6 R3 dated May 9, 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:

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 Final Audit Report dated [REDACTED] states that the Responsible Entity "did not implement processes to deter, detect, or prevent malicious code intrusions on certain of its [AIX-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 Mitigation Plan:

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], which are Electronic Access Control Monitoring Systems (EACMS) supporting [REDACTED] 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), including those involved with the performance of the [REDACTED] function, are working collaboratively on the milestone activities in this Mitigation Plan. Personnel from Information Technology (IT), [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



## NON-PUBLIC AND CONFIDENTIAL INFORMATION

has been redacted from this public version

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:



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 to this Mitigation Plan, with [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 bad [REDACTED] microcontrollers, and six (6) [REDACTED], which are EACMS supporting [REDACTED] 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 of [REDACTED] compliance 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 Requirement [REDACTED] ly, 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. [REDACTED]

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. [REDACTED]

### 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 Reliability Corporation (NERC CMEP))

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

- 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

[REDACTED] Single Point of Contact (SPOC)



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 all supporting evidence will be uploaded to the [REDACTED]

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

Completion Summary and all supporting evidence will be uploaded to the [REDACTED]

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.

[REDACTED] Mitigation Plan Verification

1: Create an inventory list of policies, standards, procedures, and work instruction documentation for malicious code prevention currently in effect for Information Technology (IT), [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 malicious code prevention implementation evidence templates not previously identified in milestone 1 for IT, [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 malicious code prevention implementation evidence templates in the inventory list created in milestone 2 for IT, [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 IT, [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 IT, [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 ensure this is documented also. The output will be a comprehensive inventory of devices with the capability of detecting, deterring, or preventing malicious code, and those that are not capable of malicious code prevention. 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 [REDACTED]. 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 – CEII" 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.



[REDACTED]

[REDACTED] staff completed their review of the evidence and verified [REDACTED] completed the Mitigation Plan by 8/17/2018.

## Attachment 11

- 11a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-007-3a R5 submitted June 19, 2018
- 11b. The Entity's Certification of Mitigation Plan Completion for CIP-007-3a R5 submitted December 31, 2018
- 11c. The Entity's Verification of Mitigation Plan Completion for CIP-007-3a R5 dated May 9, 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 &amp; 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:

In the final audit report dated [REDACTED] it stated 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 EAMS 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.







management system roles in [REDACTED]. Verify that access to CIP [REDACTED] devices is granted through access management roles. Create new roles if discrepancies are identified. Assign appropriate personnel to any new role once confirmed they are eligible and have a business need. Notify [REDACTED] of any compliance issues discovered. 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 [REDACTED] devices, and mapping all roles from the CIP [REDACTED] device to the access management system roles in [REDACTED]. Verify that access to CIP [REDACTED] devices is granted through access management roles. Create new roles if discrepancies are identified. Assign appropriate personnel to any new role once confirmed they are eligible and have a business need. Notify [REDACTED] of any compliance issues discovered. 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 [REDACTED] 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 [REDACTED] devices, and mapping all roles from the CIP [REDACTED] device to the access management system roles in [REDACTED]. Verify that access to CIP [REDACTED] devices is granted through access management roles. Create new roles if discrepancies are identified. Assign appropriate personnel to any new role once confirmed they are eligible and have a business need. Notify [REDACTED] of any compliance issues discovered.

#### 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):







This item was signed by [REDACTED] on 12/31/2018

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 [REDACTED] clearly defined roles. Working with the results [REDACTED] pages 16 and 19, identify the enterprise-wide access matrix requirements, (including how [REDACTED] changes 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 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 [REDACTED] Access Control List (ACL). Identify the new process and/or tool to be used to extract [REDACTED] 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 Completed (Due: 10/5/2018 and Completed 10/5/2018)

[Attachments \(0\)](#)

Perform an Extent of Condition (EOC) by identifying all CIP [REDACTED] devices, and mapping all roles from the CIP [REDACTED] device to the access management system roles in EAMS. Verify that access to CIP [REDACTED] devices is granted through access management roles. Create new roles if discrepancies are identified. Assign appropriate personnel to any new role once confirmed they are eligible and have a business need. Notify [REDACTED] of any compliance issues discovered.

### [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:

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

All milestone activities have been completed and the evidence for Milestones 1 through 25, plus the Completion Summaries has been uploaded to the [REDACTED]

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

All milestone activities have been completed and the evidence for Milestones 1 through 25, plus the Completion Summaries has been uploaded to the [REDACTED]

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.



## **[REDACTED] Mitigation Plan Verification**

1: Create an inventory list of policies, standards, procedures, and work instruction documentation for system access control currently in effect for Information Technology (IT), [REDACTED]

[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 IT, [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 system access control implementation evidence templates in the inventory list created in milestone 2 for IT, [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 IT, [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 IT, [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, 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 [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 [REDACTED] devices, and mapping all roles from the CIP [REDACTED] device to the access management system roles in EAMS. Verify that access to CIP [REDACTED] devices is granted through access management roles. Create new roles if discrepancies are identified. Assign appropriate personnel to any new role once confirmed they are eligible and have a business need. Notify [REDACTED] of any compliance issues discovered. To be completed by June 2, 2018.

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 [REDACTED] devices, and mapping all roles from the CIP [REDACTED] device to the access management system roles in EAMS. Verify that access to CIP [REDACTED] devices is granted through access management roles. Create new roles if discrepancies are identified. Assign appropriate personnel to any new role once confirmed they are eligible and have a business need. Notify Regional Entities 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.

[REDACTED]

[REDACTED] staff completed their review of the evidence and verified [REDACTED] completed the Mitigation Plan by 12/31/2018.

## 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 Entity's Verification of Mitigation Plan Completion for CIP-007-6 R4 dated May 9, 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 &amp; 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:

In the Final Audit Report dated [REDACTED] it stated the Responsible Entity, "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.

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 [REDACTED] 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 Information Technology (IT), [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 Information Technology (IT), [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 IT, [REDACTED] BUs. The output will be an inventory [REDACTED] templates by name/number, BU [REDACTED] 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 IT, [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 IT, [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 IT, [REDACTED] is usable and can be combined into corporate-wide documentation. Completed by September 15, 2017.

[REDACTED] 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 [REDACTED] the [REDACTED]

- 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)

HAS BEEN REDACTED FROM TH

N

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 Responsible Entity took a complete [REDACTED] 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], which are EACMS supporting [REDACTED] 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]. Actively, 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.

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

**ALL CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS DOCUMENT**

SECTION G: REGIONAL ENTITY CONTACT

[REDACTED] Single Point of Contact (SPOC)



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

R4.

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 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 all supporting evidence will be uploaded to the [REDACTED]

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

Completion Summary and all supporting evidence will be uploaded to the [REDACTED]

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.

██████████ Mitigation Plan Verification

1: Create an inventory list of policies, standards, procedures, and work instruction documentation for security event monitoring currently in effect for Information Technology (IT), ██████████ ██████████ 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 event monitoring implementation evidence templates not previously identified in milestone 1 for IT, ██████████ 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 event monitoring implementation evidence templates in the inventory list created in milestone 2 for IT, ██████████ 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 IT, ██████████ 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 IT, ██████████ 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 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. 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 [REDACTED]. 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.

[REDACTED]

[REDACTED] staff completed their review of the evidence and verified [REDACTED] completed the Mitigation Plan by 8/17/2018.

## Attachment 13

- 13a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-010-2 R2 submitted May 23, 2018
- 13b. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R2 submitted May 29, 2018
- 13c. The Entity's Verification of Mitigation Plan Completion for CIP-010-2 R2 dated August 21, 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 &amp; 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:

The final audit report dated [REDACTED] found that the Responsible Entity "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 Mitigation Plan:

The Responsible Entity to performs [REDACTED] functions for the reliable operation of the BES. 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, 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:

CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS SECTION

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 [REDACTED] 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):

The successful completion of this Mitigation Plan at SMEs have formalized documented procedures 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

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE  
D CONFIDENTIAL INFO  
HAS BEEN REDACTED FROM THIS DOCUMENT

SECTION G: REGIONAL ENTITY CONTACT

[REDACTED] Single Point of Contact (SPOC)

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 and all evidence has been uploaded to the [REDACTED]

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

Completion Summaries and all evidence has been uploaded to the [REDACTED]

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.



██████████ Mitigation Plan Verification

██ Mitigation Plan Validation

██████████

To mitigate the violation and prevent its recurrence ██████ agreed to the following:

0. Perform preliminary assessment of root cause.
1. Perform an Extent of Condition Analysis.
2. Develop narrative for enhancements by scripting the specific steps to be performed by Subject Matter Experts when baseline inconsistencies are observed.
3. Incorporate the enhancements developed in Milestone 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.
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.
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.
6. Communicate and disseminate documentation enterprise-wide by notifying impacted personnel of updates to documentation. Ensure new documentation is posted on ██████████ and related previous versions of documentation are retired.
7. Mitigate any Deficiencies Found during Completion of Previous Milestone Activities.

As evidence that the Mitigation Plan was completed the following evidence was submitted and reviewed by ██████ staff:

0. ██████ Attestation 20180515.pdf; Attestation for CIP-010 R2 Mitigation Plan, Dated 5/15/2018, shows entity attestation that the preliminary assessment of root cause was completed by 8/1/2017, and describes the identified causes.
1. Entity provided multiple files as evidence of this milestone:
  - a. IM-CIP-010-EVD-EOC\_MS1.xlsx; Undated Microsoft Excel Workbook, Spreadsheet 1 – High Impact Systems, shows listing of all entity's high impact BES Cyber Systems (BCS) and the device types found in each. Spreadsheet 2 – System-Procedure Mapping, Column C, shows listing of the CIP-010 procedure documents that apply to the devices listed in spreadsheet 1.

- b. MS01\IM-CIP-010-PRO-\*.docx; show the procedure documents identified in the above-cited Excel Workbook.
2. CIP-010 R2 MS02 [REDACTED] Completion Summary.docx; Summary of Completed Milestone Activity, Undated, shows the narratives that were proposed to be incorporated into the documents identified in milestone 1.
3. MS03\IM-CIP-010-PRO-\*.docx; show evidence the narratives documented during milestone 2 have been incorporated into the CIP-010 procedure documents identified during milestone 1. The exception is IM-CIP-010-PRO-TS KVM, which is being retired, as the device type to which it applied has been retired.
4. MS04\IM-CIP-010-PRO-\*.docx; show evidence the updated CIP-010 procedure documents from milestone 3 were approved on 12/7/2017, each with an Effective Date of 1/31/2018.
5. Entity provided multiple files as evidence of this milestone:
  - a. IT-CIP-010-EVD-EAMS-ActiveAccessReport\_20180111-CEIL.xlsx; Undated spreadsheet, shows report which was used to identify all employees with CIP roles. This system-generated report was cross-checked against the list of employees and contractors who might perform Configuration Monitoring activities to determine who should attend the online training session.
  - b. IT-CIP-010-EVD-TrainingRoster-CEIL.xlsx; Undated Microsoft Excel workbook, "IT Device Report" spreadsheet, shows list of employees and contractors who were assigned CIP roles and could potentially perform Configuration Monitoring activities, and were thus required to complete the online training session. "Training Roster" spreadsheet shows the date and time each required individual attended the scheduled online training session, the last being on 1/19/2018.
  - c. IT-CIP-010-EVD-Training\*.pdf; show evidence of attendees at each scheduled training session, as well as a one-on-one training session.
  - d. IT-CIP-010-EVD-010-2\_ProcedureUpdates.pptx; Research & report requirements for baseline deviations, Dated 1/16/2018, shows content of training from the above-referenced training sessions.
6. Entity provided multiple files as evidence of this milestone:
  - a. MS06\IM-CIP-010-PRO-\*.docx; show evidence the updated CIP-010 procedure documents from milestone 3 were approved on 12/7/2017, each with an Effective Date of 1/31/2018.
  - b. IT-CIP-010-EVD-ProcedureUpdate-SME-20180131-CEIL.pdf; Email from [REDACTED], Dated 1/30/2018, communicates the January 31, 2018 official implementation date for the CIP-010 Configuration Management Procedures, and disseminates in the form of a reminder that the updated procedures will be available via the [REDACTED].
  - c. IT-CIP-010-EVD-ProcedureUpdate-MGR-20180131-CEIL.pdf; Email from [REDACTED] to managers, Dated 1/30/2018, communicates the January 31, 2018 official implementation date for the CIP-010 Configuration Management Procedures, and disseminates in the form of a reminder that the updated procedures will be available via the [REDACTED].



7. IM-CIP-010-EVD-EOC\_MS7-CELL.xlsx; Summary of Milestone #7 analysis, Undated Microsoft Excel workbook, "Summary" spreadsheet, summarizes the steps used to determine whether any deficiencies were found while completing the previous milestones, and concludes that there were no new deficiencies requiring mitigation.

On 8/21/2018 [REDACTED] staff completed their review of the evidence and verified [REDACTED] completed the Mitigation Plan by 2/28/2018.

## Attachment 14

- 14a. The Entity's Mitigation Plan designated as [REDACTED] for CIP-011-2 R1 submitted May 23, 2018
- 14b. The Entity's Certification of Mitigation Plan Completion for CIP-011-2 R1 submitted August 8, 2018
- 14c. The Entity's Verification of Mitigation Plan Completion for CIP-011-2 R1 dated May 9, 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 &amp; 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:

The final audit report dated [REDACTED] of the Responsible Entity (RE) found that 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, where the [REDACTED] function is performed. 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 Mitigation Plan:

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 [REDACTED] 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 implement with respect to this Mitigation Plan has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

CONFIDENTIAL INFO  
HAS BEEN REDACTED FROM THIS DOCUMENT

- 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 [REDACTED]. 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]. Completed by December 20, 2017.
- 5: Address any EOC findings by: (1) Creating any necessary additional EAMS 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 [REDACTED] 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 [REDACTED]s 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 3/30/2018)

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 [REDACTED] 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 [REDACTED] application, which includes baseline and security configuration data for High Impact BES Cyber Assets in the System Control Center used for the [REDACTED] functions. 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.

There was very low risk of unauthorized access to the [REDACTED] server because multi-layered protections were in place that mitigated any risk associated with the server not being identified as a BCSI Storage Location.

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 [REDACTED] 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):

Upon completion of this Mitigation Plan, the Responsible Entity will have in place 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 annually. Messages/reminders 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 [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

[REDACTED] Single Point of Contact (SPOC)



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

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 [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 [REDACTED] 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 3/30/2018)

[Attachments \(0\)](#)

Communicate and disseminate new [REDACTED] revised IPP documents across the enterprise

1. Notify impacted personnel of the documentation update
2. Ensure that all new, revised documents are posted on [REDACTED] and related previous revisions of documents are retired.

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

Completion Summaries and all supporting evidence was uploaded to the Enforcement folder in [REDACTED].

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

D CONFIDENTIAL INFO

HAS BEEN REDACTED FROM TH

N

Completion Summaries and all supporting evidence was uploaded to the Enforcement folder in [REDACTED].

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.



© 2006 The Authors

\_\_\_\_\_

11/11/2016

properly identified. Completed by December 4, 2017.

factors. Completed by December 7, 2017.

Program (IPP) which includes:

1. *Journal of Management Studies*, 1997, 34, 1, 1-14.

Completed by January 22, 2018.

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 [REDACTED] and related previous documents are retired. Completed by April 25, 2018.

[REDACTED]

[REDACTED] staff completed their review of the evidence and verified [REDACTED] completed the Mitigation Plan by 4/15/2018.