Attachment 9

Record documents for the violation of CIP-007-6 R2

9a. The Entities' Self-Report (SERC2017018467)

9b. The Entities' Certification of Mitigation Plan Completion submitted October 11, 2017

VIEW SELF-REPORT: CIP-007-6 R2. (COMPLETED)

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

This item was submitted by [redacted] on 10/11/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:	[redacted]
NERC Registry ID:	[redacted]
JRO ID:	[redacted]
CFR ID:	[redacted]
Entity Contact Information:	[redacted]

REPORTING INFORMATION

Applicable Standard:	[redacted]
Applicable Requirement:	[redacted]
Applicable Sub Requirement(s):	[redacted]
Applicable Functions:	[redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered:	No
Has this Possible Violation previously been reported to other Regions:	No
Date Possible Violation was discovered:	9/7/2017
Beginning Date of Possible Violation:	8/15/2017
End or Expected End Date of Possible Violation:	9/8/2017
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

On 9/7/2017, the [redacted] group discovered a possible CIP-007-6 R2.3 issue where July [redacted] security patches deemed applicable on 7/11/2017 failed to be deployed to [redacted] servers (EACMS associated with Medium Impact BES Cyber Assets/Systems) by 8/15/2017 (within 35 days of the patch evaluation completion date). Upon discovery on 9/7/2017, [redacted] patch [redacted] was applied to both [redacted] servers as of 9/8/2017, which was 24 days after the patch approval date. The servers applicable to this issue were [redacted] servers out of [redacted] devices under the [redacted] patch management process.

[redacted] uses an application from [redacted] to deploy security patches to CIP cyber assets at all [redacted] medium-impact BES substations across [redacted]. The [redacted] application is used on [redacted] servers: [redacted], which deploys patches to [redacted] and [redacted] endpoints, and 2) [redacted], which deploys patches to [redacted] endpoints. The issue was discovered during the patch deployment process for July 2017 security patches.

At the time of the issue, the [redacted] required the "applicable [redacted] Administrator and/or applicable [redacted] or equivalent group shall verify the security controls and shall install the security patch(es) on each applicable Cyber Asset within 35 calendar days after the patch evaluation is complete or within the timeframe defined in the dated mitigation plan." The root cause of this issue could be attributed to ambiguity in the Substation work practice that did not clearly define roles and responsibilities between [redacted] Administrators. The failure to implement patches occurred after [redacted] Administrator completed the patch process on the [redacted] server, and then failed to access the [redacted] server and deploy patches to [redacted]. Another [redacted] Administrator completed the patch process for [redacted] because, at the time of the issue, the responsibility for patching using the both [redacted] servers was shared.

To mitigate this issue and prevent recurrence, [redacted] modified the [redacted] to add a responsibility section to clearly identify the [redacted] Administrator roles and responsibility for patch deployment. The work practice modification clarifies the [redacted] Administrator is responsible for completing the patching procedure for all applicable [redacted] and [redacted] endpoints and the [redacted] Administrator is responsible for completing the patching procedure for all applicable [redacted] and [redacted] endpoints. The change in process will identify a primary and secondary administrator for each server, and streamline the patch process and identify those responsible for completion. In addition, training on the applicable changes to the [redacted] addressing CIP-007-6 R2.3 is also scheduled for comple ion. To determine the extent of condi ion, the [redacted] group completed a review and verified on 9/13/2017 that all applicable endpoints were patched by the required timeframe of 8/15/2017.

Are Mitigating Activities in progress or completed?	Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

1) [redacted] will apply patch [redacted] to the [redacted] [redacted] servers. Completed 9/8/2017
2) [redacted] will complete a review and verify that all applicable endpoints were patched by the required timeframe of 8/15/2017 and that all patch levels are current. Completed 9/13/2017
3) [redacted] will make improvements to the [redacted] to include defined responsibilities for the [redacted] Administrators responsible for patching [redacted] and [redacted]. Completed 9/21/2017
4) [redacted] will conduct a review / training session with [redacted] Administrators responsible for patching on applicable changes to the [redacted] Work Practice addressing CIP-007-6 R2.3. Completed 10/5/2017
5) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Complete by 10/13/2017

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

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

10/13/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Closure Package	10/13/2017	[redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review.	No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue posed a minimal potential risk, and not a serious or substantial risk to the reliability of the bulk electric system. Potential risk could include the introduction of unknown vulnerabilities susceptible to exploitation by not following documented processes and applicable security patches not being in place. The root cause of this issue was a failure to thoroughly follow the security patch management steps to ensure applicable security patches are applied in a timely manner, which could be attributed to imprecise direction detailed in business unit work practices.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk, and not a serious or substantial risk to the reliability of the bulk electric system. [redacted] failure to properly follow proper patching procedures could have allowed unknown security vulnerabilities in software which could be exploited, potentially rendering one or more of these [redacted] servers inoperable. These [redacted] servers are used for BCA/S log aggregation, and any inoperability would have impacted [redacted] ability to monitor for and generate alerts in accordance with CIP-007-6 R4, but it would not have had a direct impact on BES Cyber Assets or Systems at the same locations. The [redacted] [redacted] servers are physically protected within a PSP, and other logical protections in place further minimized the actual possibility of unauthorized access or introducing malicious code on these devices. Additionally, the [redacted] product also is used to deploy device whitelisting which further prevents the introduction of malicious code on these devices. The scope of non-compliance was 24 days, and occurred on only [redacted] out of [redacted] devices under the [redacted] patch management process.

Additional Comments:

[redacted] CIP PRODECURES MANUAL:
This potential issue is considered a failure to follow [redacted] NERC CIP procedure [redacted] and the [redacted]

[redacted] Every 35 Calendar Days
c. If the Security Patch is determined to be an Applicable Security Patch, determine one of the following dispositions: 1) create a change management case to install the patch, or 2) document a new or revise an existing mitigation plan with timeframes that address the vulnerability. One of these steps must be completed within 35 calendar days from the determination of an Applicable Security Patch. Required attributes are documented in section 5.6, Evidence for Each Security Patch Mitigation Plan.

d. Personnel shall maintain a repository of security patch notices for each Security Patch Source with the date of availability, date of evaluation, and the results of the evaluation. Required attributes are documented in section 5.5,
Evidence for Each Security Patch.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW MITIGATION PLAN CLOSURE: CIP-007-6 (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 10/11/2017

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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.	SERC2017-402870	

Date of completion of the Mitigation Plan:

[redacted]

Closure Package

Milestone Pending (Due: 10/13/2017)
Attachments (0)

[redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review.

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

Description of Mitigating Activities: 1) [redacted] will apply patch [redacted] to the [redacted] servers. Completed 9/8/2017
2) [redacted] will complete a review and verify that all applicable endpoints were patched by the required timeframe of 8/15/2017 and that all patch levels are current. Completed 9/13/2017
3) [redacted] will make improvements to the [redacted] to include defined responsibilities for the [redacted] Administrators responsible for patching [redacted]. Completed 9/21/2017
4) [redacted] will conduct a review / training session with [redacted] Administrators responsible for patching on applicable changes to the [redacted] addressing CIP-007-6 R2.3. Completed 10/5/2017
5) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Complete by 10/13/2017

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

[redacted], provides screen shots demonstrating the [redacted] was applied to both the [redacted] servers, completed 9/8/2017.

[redacted] provides screen shots demonstrating a review and verification all applicable endpoints were patched using the [redacted]) and [redacted] servers. The review was completed on 9/13/2017.

[redacted] provides the previous [redacted] that did not clearly define specific responsibilities for the [redacted] Administrators responsible for patching [redacted] endpoints at all [redacted] endpoints.

[redacted]), provides the updated [redacted] which includes more clearly defined responsibilities for the [redacted] Administrators responsible for patching [redacted] endpoints at all [redacted] endpoints. Completed 9/21/2017.

[redacted] Page 1 provides the meeting notice where [redacted] conducted a review session with [redacted] Administrators at [redacted]. Page 3 provides meeting notes documenting; 1) changes to the [redacted] to include more clearly defined responsibilities for the [redacted] Administrators responsible for patching [redacted] endpoints, 2) Primary and secondary [redacted] Administrators assigned for the [redacted] servers, and 3) a review of the CIP-007-6 R2.3 standard requirements and timeframes. The review was completed on 10/5/2017.

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.

Attachment 10

Record documents for the violation of CIP-007-6 R3

10a. The Entities' Self-Report (SERC2017017236)

10b. The Entities' Mitigation Plan designated as SERCMIT014396 submitted July 10, 2018

10c. The Entities' Certification of Mitigation Plan Completion submitted July 10, 2018

VIEW SELF-REPORT: CIP-007-6 R3. (COMPLETED)

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

This item was submitted by [redacted] on 3/16/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:	[redacted]
NERC Registry ID:	[redacted]
JRO ID:	[redacted]
CFR ID:	[redacted]
Entity Contact Information:	[redacted]

REPORTING INFORMATION

Applicable Standard:	[redacted]
Applicable Requirement:	[redacted]
Applicable Sub Requirement(s):	[redacted]
Applicable Functions:	[redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered:	No
Has this Possible Violation previously been reported to other Regions:	No
Date Possible Violation was discovered:	12/5/2016
Beginning Date of Possible Violation:	10/2/2016
End or Expected End Date of Possible Violation:	2/7/2017
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

On December 5, 2016, the [redacted] group discovered a possible violation of CIP-007-6 R3.1 when it was determined that a vendor solution [redacted] implemented to enforce whitelisting on applicable devices to meet the security objectives of deterring, detecting, and preventing malicious code had stopped working. This issue was discovered after the hard drives in [redacted] servers were re-imaged due to issues with those drives, and the [redacted] personnel were confirming security controls checks following the change. A review of the vendor product [redacted] was performed that indicated whitelist rules were enabled and being enforced on the [redacted] endpoint servers, however, a review of the endpoint servers themselves revealed that software not in the whitelist could be run. The [redacted] endpoint servers are [redacted] EACMS associated with Transmission Substation Medium Impact BES Cyber Systems, and are used to support logging and security event monitoring in accordance with CIP-007-6 R4. Additionally, upon investigation, the vendor product [redacted] showed that the last policy refresh for these [redacted] servers was successfully deployed on October 2, 2016.

To determine the extent of condition, the [redacted] group checked all other [redacted] EACMS servers across [redacted] by testing the endpoint servers and confirming the whitelist was enabled and was currently up to date, and that the whitelist was working correctly and properly enforced on those servers. To mitigate this issue, [redacted] and [redacted] IT compared the [redacted] servers used to enforce whitelisting on all [redacted] EACMS servers across [redacted] to ensure there were no discrepancies that would lead to the whitelist working on one but not the other. As of January 17, 2017, [redacted] IT completed its review and found the configuration and implementation of both [redacted] servers to be identical. [redacted] began working with the [redacted] vendor [redacted] software) to determine why the [redacted] application indicated the whitelists were enabled and enforcing malicious code prevention on each of the [redacted] EACMS servers, however failing to work or update. Additionally, on December 21, 2016, [redacted] disabled all Interactive Remote Access to these [redacted] servers to further harden those devices to reduce risk while resolution with the vendor was in progress. On February 7, 2017, [redacted] and the [redacted] vendor discovered here were corrupted configuration files in the [redacted] server. Once those files were removed, [redacted] successfully deployed the whitelisting policy to the [redacted] servers.

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

1) [redacted] will complete an extent of condition review of the functionality of the [redacted] whitelisting on the [redacted] devices on the second [redacted] server to confirm whitelisting is enabled and properly enforcing device whitelists for [redacted] and [redacted] devices. (Completed 12/5/2016).
2) [redacted] will disable Interactive Remote Access capability to the [redacted] servers to temporarily harden these devices and prevent external remote access until resolution with the vendor can be achieved. (Completed 12/21/2016)
3) [redacted] working with [redacted] IT and the contracted vendor, will confirm that whitelisting rules have been re-enabled and are functioning properly to deter, detect, and

prevent malicious code on affected devices. (Completed 3/14/2017)
4) [redacted] will review Substation work practices and determine if any updates or corrections could be made to help with troubleshooting and/or identifying this issue in a timelier manner. (Completed 3/15/2017)

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

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

3/15/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue posed a minimal potential risk, and not a serious or substantial risk to the reliability of the bulk electric system. Due to the [redacted] whitelist failing to restrict the ability to run unauthorized software on these devices as designed, an external user with remote access into the [redacted] servers could have allowed the introduction of malicious code prior to remote access to these devices being removed on December 21, 2016. Additionally, a user authorized for unescorted physical access to the PSPs containing these [redacted] EACMS servers could have accessed these devices with the ability to potentially launch malicious code while the whitelisting function was not being enforced.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk, and not a serious or substantial risk to the reliability of the bulk electric system. The failure of the [redacted] product to enforce device whitelisting to deter, detect, or prevent malicious code could have allowed a user with authorization for physical access to the Substation PSP or remote access to the [redacted] servers the ability to run unauthorized software or potentially introduce malicious code onto EACMS devices used for security event monitoring. Potentially rendering one or more of these [redacted] EACMS servers inoperable due to the introduction of malicious code would have impacted [redacted] ability to monitor for and generate alerts in accordance with CIP-007-6 R4, but would not have had a direct impact on BES Cyber Assets or Systems at the same locations. After initial troubleshooting and investigation, remote access to these [redacted] EACMS servers was removed on December 21, 2016 to further reduce the risk of compromise or the possibility for the introduction of malicious code. All of the [redacted] EACMS servers are physically protected within a PSP, and other logical protections in place further minimized the actual possibility of running unauthorized software or introducing malicious code on these devices.

Additional Comments:

[redacted]

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW FORMAL MITIGATION PLAN: CIP-007-6 (REGION REVIEWING MITIGATION PLAN)

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

This item was signed by [redacted] on 7/10/2018

This item was marked ready for signature by [redacted] on 7/10/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-007-6 R3.	SERC2017017236	SERC2017-402643	03/16/2017	Revision Requested	Informal	
CIP-007-6 R3.	SERC2017017236	SERC2017-402643	07/10/2018	Region reviewing Mitigation Plan	Formal	1

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

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

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

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name: [redacted]

Company Address: [redacted]

[redacted]

Compliance Registry ID: [redacted]

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

Name: [redacted]

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

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

Standard: [redacted]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R3.	SERC2017-402643	SERC2017017236	3/16/2017

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

On December 5, 2016, the [redacted] group discovered a possible violation of CIP-007-6 R3.1 when it was determined that a vendor patch management and whitelisting solution [redacted] implemented to meet the security objectives of deterring, detecting, and preventing malicious code had stopped working. This issue was discovered after the hard drives in [redacted] servers were re-imaged due to issues with those drives, and the [redacted] personnel were confirming security controls checks following the change. A review of the vendor product [redacted] was performed that indicated whitelist rules were enabled and being enforced on the [redacted] endpoint servers; however, a review of the endpoint servers themselves revealed that software not in the whitelist provided by the vendor could be run. The [redacted] endpoint servers are [redacted] EACMS associated with Transmission Substation Medium Impact BES Cyber Systems, and are used to support logging and security event monitoring in accordance with CIP-007-6 R4. Additionally, upon investigation, the vendor product [redacted] showed that the last policy refresh for these [redacted] servers was successfully deployed on October 2, 2016.

The root-cause of this issue was assessed to be a software failure with the [redacted] application. The whitelisting policies within the application on the [redacted] server failed to deploy properly and to enforce whitelisting on endpoint devices. Vendor support was needed to determine the cause of this issue, and mitigation resulted in the deletion and recreation of the necessary installation files and applicable whitelist policies to enforce malicious code prevention.

To determine the extent of condition, the [redacted] group checked all other [redacted] EACMS servers across [redacted] by testing the endpoint servers and confirming the whitelist was enabled and was currently up to date, and that the whitelist was working correctly and properly enforced on those servers. To mitigate this issue, [redacted] and [redacted] IT compared the [redacted] servers used to enforce whitelisting on all [redacted] EACMS servers across [redacted] to ensure there were no discrepancies that would lead to the whitelist working on one but not the other. As of January 17, 2017, [redacted] IT completed its review and found the configuration and implementation of both [redacted] servers to be identical. [redacted] began working with the [redacted] vendor [redacted] to determine why the [redacted] application indicated the whitelists were enabled and enforcing malicious code prevention on each of the [redacted] EACMS servers, however failing to work or update. Additionally, on December 21, 2016, [redacted] disabled all Interactive Remote Access to these [redacted] servers to further harden those devices to reduce risk while resolution with the vendor was in progress. On February 7, 2017, [redacted] and the [redacted] vendor discovered there were configuration files that were either corrupted or did not install properly during the drive re-imaging process for the [redacted] server. Once those files were removed, they were successfully reinstalled and the [redacted] server successfully deployed the whitelisting policy to the [redacted] servers.

There was no known harm that occurred as a result of this issue.

Attachments ()

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

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

[redacted] uses a [redacted] Software product named [redacted] to enforce whitelisting on Substation endpoint devices to comply with CIP-007-6 R3 for malicious code prevention. Substation endpoint devices include BES Cyber Assets/Systems, EACMS, and PCAs. In this particular issue, the endpoint devices where whitelisting enforcement failed were only [redacted] EACMS devices used for log aggregation and correlation of logs from Substation Medium Impact BES Cyber Systems (i.e., the whitelist issues were not impacting any BES Cyber Assets/Systems or PCAs – just the EACMSs used to collect their logs).

There are currently [redacted] servers used as management consoles to push whitelisting rules to these Substation [redacted] EACMS devices; one server is used to push whitelisting rules and enforcement to [redacted] endpoint devices in [redacted] and [redacted] Substations, [redacted]; the second is used to push whitelisting rules and enforcement to [redacted] endpoint devices in [redacted] and [redacted] Substations, [redacted] The [redacted] server and its associated endpoint devices were not affected.

This issue involved [redacted] and [redacted] EACMS cyber assets out of a total of [redacted] EACMS cyber assets associated with Transmission Substations medium impact BES Cyber Systems across [redacted]. At the time of this issue, there were [redacted] Transmission Substations medium impact BES Cyber Assets/Systems, [redacted] EACMS, and [redacted] PCAs across [redacted] The [redacted] and [redacted] application servers are not in scope as an applicable Cyber Asset. These devices are used to configure and deploy whitelisting rules used to enforce malicious code prevention on in-scope EACMS Cyber Assets using only a system-to-system communication method.

A timeline of events associated with this issue is as follows:
• October 2016: [redacted] experienced problems installing patches on some [redacted] endpoint devices. To correct this issue, [redacted] re-imaged these device hard drives to correct this issue.

• December 5, 2016: After re-imaging the hard drives, [redacted] discovered that the reimaged [redacted] (EACMS) endpoint devices connected to the [redacted] server were not properly enforcing whitelist rules. A review of the [redacted] application reported whitelisting was enabled; however, it was discovered during security control testing at the endpoints that scripts/applications not in the whitelist were not being blocked. This occurred on [redacted] endpoint [redacted] devices at [redacted] medium Substations and [redacted] medium Substations.

[redacted] completed a review using the [redacted] server and found that after the drives were re-imaged in October, whitelisting was working correctly on those servers and their associated endpoint devices.

• December 21, 2016: As a result of the whitelisting issue, [redacted] disabled Interactive Remote Access to the [redacted] endpoint [redacted] EACMS devices connected to the [redacted] server to further harden access to those devices, and reduce risk while they worked with the vendor to determine the root cause of the whitelisting issue.

• January 17, 2016 [redacted] IT was unable to identify the reason why the whitelist rules were working for the [redacted] server but not the [redacted] server. [redacted] worked with the [redacted] vendor, [redacted] to share their internal troubleshooting results.

• February 7, 2017: [redacted] and [redacted] determined the whitelist policy files on the [redacted] server were either corrupted or did not install properly when the drives were re-imaged. These policy files are proprietary to the application, and once deleted the [redacted] application recreated the policy files using the whitelisting configuration on the server. The new policy files worked properly and were successfully pushed to [redacted] endpoint devices, enabling the enforcement of malicious code prevention.

• March 14, 2017: The [redacted] endpoint device was offline between 2/7/2017 and 3/14/2017 due to vendor maintenance. Once the [redacted] device was put back online, [redacted] successfully pushed whitelisting policies from the [redacted] server to the device, enabling the enforcement of malicious code prevention.

As part of the [redacted] CIP Procedures Manual, [redacted] has implemented the [redacted], [redacted] procedure to address CIP-007-6 R3.1. [redacted] addresses the lifecycle of applicable CIP Cyber Systems. This procedure takes all of the various requirements associated with the technical management of cyber assets or cyber systems and organizes these tasks by the lifecycle stage of the applicable system for ease of use by support personnel. It includes the steps to follow for planning for a new CIP Cyber System (Section 4.1), commissioning a new CIP Cyber Systems (Section 4.2), maintaining existing CIP Cyber Systems including tasks performed at varying periodicity throughout the system's lifetime (Section 4.3), and decommissioning CIP Cyber Systems (Section 4.4).
• Planning stage - Section 4.1, Step 3 requires the determination of the method(s) to be used to deter, detect, or prevent malicious code on a CIP Cyber System.
• Commissioning stage - Section 4.2, Step 6 requires the validation of method(s) determined in section 4.1 prior to commissioning.

This issue was caused by a vendor product malfunction. There was not a specific procedure or work practice that was not followed that resulted in a potential violation.

This issue was not discovered through a formal internal controls process; however, the issue was discovered when security control checks were performed in accordance with CIP-010-2 R1.4 after the hard drives on endpoint devices were re-imaged.

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:

Description of Mitigating Activities:
1) [redacted] will complete an extent of condition review of the functionality of the [redacted] whitelisting on the [redacted] devices on the [redacted] server to confirm whitelisting is enabled and properly enforcing device whitelists for [redacted] and [redacted] devices. (Completed 12/5/2016).
2) [redacted] will disable Interactive Remote Access capability to the [redacted] servers to temporarily harden these devices and prevent external remote access until resolution with the vendor can be achieved. (Completed 12/21/2016)
3) [redacted] working with [redacted] IT and the contracted vendor, will confirm that whitelisting rules have been re-enabled and are functioning properly to deter, detect, and prevent malicious code on affected devices. (Completed 3/14/2017)
4) [redacted] will review Substation work practices and determine if any updates or corrections could be made to help with troubleshooting and/or identifying this issue in a timelier manner. (Completed 3/15/2017)

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

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:

3/15/2017

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, 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):

(i) There are no known additional risks or impacts to the BPS while the actions in this mitigation plan are being completed.
(ii) [redacted] does not plan to implement additional actions that would increase risks to the reliability of the BPS as part of this mitigation plan.

[redacted] assesses this issue posed a minimal actual risk, and not a serious or substantial risk to the reliability of the bulk electric system. The failure of the [redacted] product to enforce device whitelisting to deter, detect, or prevent malicious code could have allowed a user with authorization for physical access to the Substation PSP or remote access to the [redacted] servers the ability to run unauthorized software or potentially introduce malicious code onto EACMS devices used for security event monitoring. Potentially rendering one or more of these [redacted] EACMS servers inoperable due to the introduction of malicious code would have impacted [redacted] ability to monitor for and generate alerts in accordance with CIP-007-6 R4, but would not have had a direct impact on BES Cyber Assets or Systems at the same locations. After initial troubleshooting and investigation, remote access to these [redacted] EACMS servers was removed on December 21, 2016 to further reduce the risk of compromise or the possibility for the introduction of malicious code. All of the [redacted] EACMS servers are physically protected within a PSP, and other logical protections in place further minimized the actual possibility of running unauthorized software or introducing malicious code on these devices.

In addition, only [redacted] and [redacted] employees have approved Interactive Remote Access to these [redacted] EACMS devices, and electronic access to the respective shared account passwords for these [redacted] EACMS devices. Of those [redacted] and [redacted] employees, [redacted] and [redacted] had authorized unescorted physical access to [redacted] and [redacted] Substation PSPs. This further minimized the actual possibility of running unauthorized software or introducing malicious code on these EACMS devices. All of the endpoint devices associated with this issue are EACMS devices used to meet CIP-007-6 R4 by performing security event log correlation and monitoring of applicable assets within the ESP; the impacted devices are not involved in the authentication or control of electronic or Interactive Remote Access into the ESP.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitiga ion 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 will minimize the probability of future violations of the same requirements.

As noted in the originally submitted self-report, [redacted] has completed the following actions to prevent future recurrence:
4) [redacted] will review Substation work practices and determine if any updates or corrections could be made to help with troubleshooting and/or identifying this issue in a timelier manner. (Completed 3/15/2017)

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 SERC and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
  - I am [redacted] of [redacted]
  - I am qualified to sign this Mitigation Plan on behalf of [redacted]
  - I understand [redacted] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendixe 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 SERC and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

SERC Single Point of Contact (SPOC)

VIEW MITIGATION PLAN CLOSURE: CIP-007-6 (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 7/10/2018

This item was marked ready for signature by [redacted] on 7/10/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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
R3.	SERC2017-402643	SERC2017017236

Date of completion of the Mitigation Plan:

[redacted]

No Milestones Defined

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

Description of Mitigating Activities:
1) [redacted] will complete an extent of condition review of the functionality of the [redacted] whitelis ing on the [redacted] t devices on he second [redacted] server to confirm whitelisting is enabled and properly enforcing device whitelists for [redacted] and [redacted] devices. (Completed 12/5/2016).
2) [redacted] will disable Interactive Remote Access capability to the [redacted] servers to temporarily harden these devices and prevent external remote access until resolution with the vendor can be achieved. (Completed 12/21/2016)
3) [redacted] working with [redacted] IT and the contracted vendor, will confirm that whitelisting rules have been re-enabled and are functioning properly to deter, detect, and prevent malicious code on affected devices. (Completed 3/14/2017)
4) [redacted] will review Substation work practices and determine if any updates or corrections could be made to help with troubleshooting and/or identifying this issue in a timelier manner. (Completed 3/15/2017)

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

Milestone 1:
[redacted] this document provides confirmation as of 12/5/2016 that whitelisting was enabled and active on the [redacted] endpoint devices associated with the [redacted] server, after the hard drives were reimaged. This confirmed that the whitelist enforcement issue was limited to the [redacted] server.

Milestone 2:
[redacted] this document provides confirmation IRA was disabled as of 12/21/2016 on the [redacted] devices associated with the [redacted] server. IRA was disabled to temporarily harden the devices and prevent external remote access while issues with the [redacted] server were resolved with the vendor.

Milestone 3:
[redacted] this document provides screen capture evidence on pages 2-21 showing the whitelisting functionality was corrected and re-enabled for [redacted] of the [redacted] endpoint devices on 2/7/2016, and on 3/14/2016 for the [redacted] device enforced by the [redacted] server.

Milestone 4:
[redacted] ; this document is the updated [redacted], which includes, on page 1, an added section 3.1, Step 3, instruction to the [redacted] Administrator to disable Interactive Remote Access (IRA) to the device in the event the whitelisting function fails. Once the whitelisting function has been restored, IRA can be re-enabled. The change log, describing the edits made on 2/9/2017 and approved on 2/15/2017, is on page 4 of this document.

[redacted], this document provides an email notification as of 3/15/2016 to the [redacted] Administrators and those who suppor [redacted] an update to the [redacted] was made regarding whitelisting.

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.

Attachment 11

Record documents for the violation of CIP-007-3a R5

11a. The Entities' Self-Report (SERC2017016832)

11b. The Entities' Mitigation Plan designated as SERCMIT014423 submitted February 8, 2019

11c. The Entities' Certification of Mitigation Plan Completion submitted February 8, 2019

VIEW SELF-REPORT: CIP-007-3A R5. (COMPLETED)

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

This item was submitted by [redacted] on 1/25/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:	[redacted]
NERC Registry ID:	[redacted]
JRO ID:	[redacted]
CFR ID:	[redacted]
Entity Contact Information:	[redacted]

REPORTING INFORMATION

Applicable Standard:	[redacted]
Applicable Requirement:	[redacted]
Applicable Sub Requirement(s):	[redacted]
Applicable Functions:	[redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered:	No
Has this Possible Violation previously been reported to other Regions:	No
Date Possible Violation was discovered:	8/31/2016
Beginning Date of Possible Violation:	11/30/2011
End or Expected End Date of Possible Violation:	11/22/2016
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

While responding to a SERC data request in preparation for [redacted] recent CIP audit, [redacted] EMS discovered on [redacted] that the passwords for [redacted] " device shared user accounts had not been changed since 5/4/2015, which was longer than "at least once every six months" in accordance with EMS policy, and also longer than the annual timeframe required by the CIP standards (CIP-007-3 R5.2/R5.3). EMS also discovered, in their investigation of this issue, [redacted] additional [redacted] devices where there was no historical evidence via change records, emails, correspondence, etc. of a bi-annual or annual password change for these device shared user accounts after they were commissioned between 5/31/2011 and 10/7/2016. All of these [redacted] devices were classified as Critical Cyber Assets under CIP V3, and as BES Cyber Assets associated with a High Impact BES Cyber System under CIP V5. These devices are used to convert data from serial to IP for transmitting data from remote [redacted] sites back to a Control Center. The passwords for the [redacted] shared user accounts on the [redacted] devices should have been changed by 11/4/2015 (6 months after 5/4/2015) in accordance with EMS policy, and by 5/4/2016 in accordance with the V3 standards, specifically CIP-007-3 R5.2/R5.3, to address risk in the event of terminated or transferred authorized users being able to access these devices. For the remaining shared account passwords on the additional [redacted] devices, no additional historical evidence could be found demonstrating a bi-annual or annual password change after 11/30/2011 (six months after the earliest recorded commissioning of those devices).

Upon discovery, password changes for shared accounts on all [redacted] current EMS [redacted] devices were completed as of 11/22/2016. [redacted] new [redacted] devices were commissioned by EMS between 9/30/2015 and 3/25/2016 and none of those [redacted] devices had yet reached the expiration of their initial default password change "at least once every 15 calendar months" in accordance with CIP V5; additionally, EMS had taken [redacted] [redacted] devices out of service as of 5/14/2016, therefore only the initial [redacted] of the [redacted] current [redacted] devices were out of compliance. The scope of the potential violation is from 11/30/2011 until 11/22/2016 (approximately 5 years). To determine the extent-of-condition of this issue, EMS reviewed evidence supporting the changing of all shared account passwords on devices other than these [redacted] cyber assets. As evidence of this comprehensive review of all EMS shared user accounts and their associated last password change date, the file [redacted] is provided to support confirmation that the [redacted] password change issue constitutes the full extent of condition for this issue.

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

1. EMS Compliance will train EMS employees on the EMS [redacted] process for managing [redacted] passwords and password changes in the [redacted] application. Completed 11/16/16
2. EMS will change all shared user account passwords on the [redacted] current EMS [redacted] devices. Completed 11/22/2016.

3. EMS will edit the [redacted] to include a reference to the EMS [redacted] used for password management of [redacted] devices going forward using the EMS [redacted] application. Completed 11/30/2016
4. EMS will transition shared account password storage and management for the [redacted] devices to the EMS [redacted] application to automate password changes in the event of personnel changes. Completed 12/5/2016
5. [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Complete by 2/17/2017

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

2/17/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Train users on [redacted]	11/16/2016	EMS Compliance will train EMS employees on the EMS [redacted] process for managing [redacted] passwords and password changes in the [redacted] application.	Yes
Change Passwords	11/22/2016	EMS will change all shared user account passwords on the [redacted] current EMS [redacted] devices.	No
Update EMS Procedures	12/5/2016	EMS will edit the [redacted] to include a reference to the EMS [redacted] used for password management of [redacted] devices going forward using the EMS [redacted] application.	Yes
Manage Asset Passwords in [redacted]	12/5/2016	EMS will transition shared account password storage and management for the [redacted] devices to the EMS [redacted] application to automate password changes in the event of personnel changes.	Yes
Submit for Closure	2/17/2017	[redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.	No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue poses a minimal potential risk, and not a serious or substantial potential risk to the bulk power system. If unauthorized disclosure, or an unauthorized user had previous knowledge of a shared user account password for one of these [redacted] devices (terminal servers), a user could potentially reboot the device or change the IP address, which could cause a temporary loss of communications between Substation field devices and the Remote Front End (RFE) devices passing data back to the EMS [redacted] system used by a Control Center. A loss of data communications would limit some of the information received by the Control Centers for a very brief period of time, but they would have access to alternate information flows for that data. In addition to having to have knowledge of the device's shared user account password, the user would also have to have either physical access authorization to the device's location, or electronic Interactive Remote Access authorization, which provide additional defense-in-depth layers to prevent compromise.

Provide detailed description of Actual Risk to Bulk Power System:

This issue poses a minimal actual risk, and not a serious or substantial actual risk to the bulk power system. The EMS business unit utilizes the EMS Support Center (ESC) as a 24/7 response center that performs constant monitoring of communications paths used by the Control Centers. Additionally, al [redacted] devices used by EMS are deployed in pairs such that if one device or its communications path is down, communications fail-over to the backup device. This fail-over process is automatic, and if automatic fail-over does not occur, fail-over can be initiated remotely by the ESC upon receiving a real-time alert that the device or the communications path is down. Routinely, EMS will plan and schedule maintenance and other tasks that will require these devices to be down for a period of time, in which case there is little to no impact to the Control Centers. EMS also maintains replacement devices that could be changed out if a device were compromised or misconfigured based on the potential issue of not changing the device's shared user account password routinely.

In order to electronically access the [redacted] devices physically (locally at the device) or remotely, a user must first have authorization in [redacted] for shared user account access to be able to log in to the device. Separate authorizations and access provisioning would be required for either physical access or Interactive Remote Access to get to the devices. When access to a [redacted] device is needed, a user must first contact the EMS Support Center (ESC) to obtain the shared user account password. The ESC first checks the current authorization list in [redacted] for approval for shared user account access, and issues shared user account passwords only to authorized personnel.

EMS uses strong passwords for all shared user accounts. The potential for electronically accessing the [redacted] devices via the shared user account is diminished by the complexity of the password. Additionally, upon discovery of this issue, a review of alerts from the EMS ESC for device or communications failures related to all [redacted] devices was conducted. During the review, it was determined that there was no previous indication or alert of unauthorized or malicious access detected during the scope of this potential issue that would have required activation of the CIP-008 Incident Response Plan.

Additional Comments:

CIP-007-3 R5.2 states "the Responsible Entity shall have a policy for managing the use of such accounts… and steps for securing the account in the event of personnel changes." Additionally, CIP-007-3 R5.3.3 states "Each password shall be changed at least annually, or more frequently based on risk." The EMS User Account Management Policy under Version 3 established a password change requirement for shared user accounts to occur at least twice per year to address this risk; however, research has indicated that there have not been adequate records kept to demonstrate the annual or bi-annual changing of the shared account passwords on these [redacted] devices.

Now, under CIP V5, additional requirements have been added to CIP-004-6 and CIP-007-6 specifically addressing the changing of shared account passwords within 30 days of the effective date of a termination or transfer of applicable personnel that no longer require such access (CIP-004-6) and at least once every 15 calendar months (CIP-007-6). [redacted] under CIP V5 now requires the changing of shared account passwords known to the user within 30 calendar days of their termination or transfer. Additionally, [redacted] NERC CIP password management process under CIP V5 is now governed by procedure [redacted] requires that where technically feasible, for single factor password-only authentication of interactive user access, a password change must be technically or procedurally enforced at least once every 15 calendar months. At the time of the audit, the [redacted] device shared user accounts provided password-only authentication of interactive user access, and password changes at least annually were being procedurally enforced. Mitigation of this issue will include the implementation of technical controls to manage and automate password changes for the shared accounts on these [redacted] devices using the EMS [redacted] application.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW FORMAL MITIGATION PLAN: CIP-007-3A (REGION REVIEWING MITIGATION PLAN)

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

This item was signed by [redacted] on 2/8/2019

This item was marked ready for signature by [redacted] on 2/8/2019

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-007-3a R5.	SERC2017016832	SERC2017-402615	01/25/2017	Revision Requested	Informal	
CIP-007-3a R5.	SERC2017016832	SERC2017-402615	02/08/2019	Region reviewing Mitigation Plan	Formal	1

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

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

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

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name: [redacted]

Company Address: [redacted]

[redacted]

Compliance Registry ID: [redacted]

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

Name: [redacted]

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

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

Standard: [redacted]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R5.	SERC2017-402615	SERC2017016832	1/25/2017

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

While responding to a SERC data request in preparation for [redacted] 2016 CIP audit, [redacted] EMS discovered on [redacted] that the passwords for [redacted] device shared user accounts had not be[redacted]/2015, which was longe[redacted]east once every six months" in accordance [redacted]S policy, and also longer than the annual time frame required by the CIP standards (CIP-007-3 R5.2/R5.3). EMS also discovered, in their investigation of this issue, [redacted] additional [redacted] devices where there was no historical evidence via change records, emails, correspondence, etc. of a bi-annual or annual password change for these device shared user accounts after they were commissioned between 5/31/2011 and 10/7/2016. All of these [redacted] devices were classified as Critical Cyber Assets under CIP V3, and as BES Cyber Assets associated w[redacted] a High Impact BES [redacted]stem under CIP V5. These devices are used to convert data from serial to IP for transmitting data from remote[redacted] sites back to a Control Center. The passwords for the [redacted] shared user accounts on the [redacted] devices should have been changed by 11/4/2015 (6 months after 5/4/2015) in accordance with EMS policy, and by 5/4/2016 in accordance with the V3 standards, specifically CIP-007-3 R5.2/R5.3, t[redacted]minated or transferred authorized u[redacted]cess these devices. For the remainin[redacted] account passwords on the addi[redacted] devices, no additional historical evidence could be found demonstrating a bi-annual or annual password change after 11/30/2011 (six months after the earliest recorded commissioning of those devices).

Upon discovery, password changes for shared accounts on all [redacted] current EMS [redacted] vices were complete[redacted]/22/2016. [redacted] new [redacted] devices were commissioned by EMS between 9/30/2015 and 3/25/2016 and none of those [redacted] devices had yet reached the expiration of their initial default password change "at least once every 15 calendar months" in accordance with CIP V5; additionally, EMS had taken [redacted] devices out of service as of 5/14/2016, therefore only the initial [redacted] of the [redacted] current [redacted] devices were out of compliance. The scope of the potential violation is from 11/30/2011 until 11/22/2016 (approximately 5 years). To determine the [redacted]ent-of-condition of this issue, EMS reviewed evidence supporting the changing of all shared account passwords on devices other than these [redacted] cyber assets. As evidence of this comprehensive review of all EMS shared user accounts and their associated last password change date, the file [redacted] is provided to support confirmation hat the [redacted] password change issue constitutes the full extent of condition for this issue.

There was no known harm that occurred as a result of this issue.

Attachments ()

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

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

Under CIP Version 3, EMS User Account Manag licy documented con s issue in Section 2.4.2- Passwords, which notes that "Shared system account passwords must be changed at least twice a year." See

This issue was not discovered through a formal internal controls process; but rather, while responding to a SERC data request in preparation for 2016 NERC CIP audit. initially became aware of a potential issue while preparing for the 2016 CIP Audit. At the time of the Audit, investigation into the issue was underway. made the SERC Audit Team aware of this potential violation prior to the start of the 2016 CIP Audit. Operations Compliance provided SERC Audit Team with documentation su al violations Self-Report SERC Portal, as well as all potential violati g investigated. This summary included an item noting that "EMS discovered shared user accounts on approximately EMS CCAs that had not had a password changed annually." This summary was provided to the SERC Audit Team on October 3, 2016. Operations Compliance also met with the SERC Audit Team Lead via teleconference on October 3, 2016 to discuss all potential violations being investigated as well as those Self-Reported on the SERC Portal. In addition, the documentation summarizing all potential violations was uplo ed to cure file transfer protocol site on October 4, 2016 Operations Compliance informed its SERC single point of contact, , of the availability of this document on October 4, 2016, which was prior to the on-site portion of the 2016 SERC CIP Audit.

The apparent root-caus human performance errors and a lack of management oversight of the performance of annual compliance tasks under CIP Version 3. Under CIP Version 3, the shared passwords were to be changed every 6 months, as outlined in the EMS User Account Management Policy, but this was not completed. The relevant employees have been retrained on updated EMS Electronic Access work practices, as documented in Mitigation Step 1 associated with this Self-Report. Additionally, EMS has transitioned shared account password storage and ment fo de he EMS application to automate password changes, as documented in Mitigation Step 4 associated with this Self-Report.
EMS relies upon its strong layered security strategy that includes infrastructure and security measures to mitigate vulnerabilities.

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:

Description of Mitigating Activities and Completion Dates:
1. E S ce trained EMS employees on the EMS process for managing passwords and password changes in the application.
   - Due: 6
   - Completed: 11/16/2016
2. EMS changed all shared user account passwords on the then current, EMS devices.
   - Due: 11/22/2016
   - Completed: 11/22/2016
3. EMS edited the to include a reference to the EMS used for password management of devices going forward using the EMS on.
   - Due: 12/05/2016
   - Completed: 11/30/2016
4. EMS transitioned shared account password storage and ma gement for th devices to the EMS applicatio autor sword changes in the event of personnel changes.
   - Due: 12/05/2016
   - mplete 2016
5. Operations Compliance completed a comprehensive review of all required evidence associated with this mitigation plan and prepared a losure packet for SERC review and settlement of this potential violation.
   - Completed 02/01/2017

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will help prevent future recurrence of this issue.

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:

2/17/2017

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

Train users on

Milestone Completed (Due: 11/16/2016 and Completed 11/16/2016)

Compliance e EMS rds and password cha e application.

Change Passwords

Milestone Completed (Due: 11/22/2016 and Completed 11/22/2016)

EMS will change all shared user account passwords on the current EMS devices.

Update EMS Procedures

Milestone Completed (Due: 12/5/2016 and Completed 11/30/2016)

will edit the to incl sword management of d ing forward using the EMS application.

Manage Asset Passwords in

Milestone Completed (Due: 12/5/2016 and Completed 12/5/2016)

[redacted] will transitio[redacted]age an[redacted] application to automa[redacted]rd[redacted]s in the event of personnel cha[redacted]

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

Submit for Closure[redacted] [redacted]

Milestone Completed (Due: 2/17/2017 and Completed 2/1/2017)

[redacted] Operations [redacted]preher[redacted]ation plan and prepare[redacted]ry[redacted]packet for SERC review and se[redacted] of this potential violation.

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):

(i) There were no known additional risks or impacts to the BPS while the actions in this mitigation plan were being completed.
(ii)[redacted] did not plan to implement additional actions that would have increased risks to the reliability of the BPS as part of this mitigation plan.

This issue posed a minimal actual risk, and not a serious or substantial actual risk to the bulk power system. The EMS business unit utilizes the EMS Support Center (ESC) as a 24/7 response center that performs constant monitoring of communications paths used by the Control Centers. Additionally, all [redacted] devices used by EMS are deployed in pairs such that if one device or its communications path is down, communications fail-over to the backup device. This fail-over process is automatic, and if automatic fail-over does not occur, fail-over can be initiated remotely by the ESC upon receiving a real-time alert that the device or the communications path is down. Routinely, EMS will plan and schedule maintenance and other tasks that will require these devices to be down for a period of time, in which case there is little to no impact to the Control Centers. EMS also maintains replacement devices that could be changed out if a device were compromised or misconfigured based on the potential issue of not changing the device's shared user account password routinely.

In order to electronically access the [redacted] devices physically (locally at the device) or remotely, a user must first have authorization in [redacted] for shared user account access to be able to log in to the device. Separate authorizations and access provisioning would be required for either physical access or Interactive Remote Access to get to the devices. When access to a [redacted] device is needed, a user must first contact the EMS Support Center (ESC) to obtain the shared user account password. The ESC first checks the current authorization list in [redacted] (the AMA) for approval for shared user account access, and issues shared user account passwords only to authorized personnel. If a user is terminated for any reason, all access is revoked in the AMA which would indicate to the ESC that the password should not be revealed to the requesting user.

EMS uses strong passwords for all shared user accounts. The potential for electronically accessing the [redacted] devices via the shared user account is diminished by the complexity of the password. Additionally, upon discovery of this issue, a review of alerts from the EMS ESC for device or communications failures related to all [redacted] [redacted] devices was conducted. During the review, it was determined that there was no previous indication or alert of unauthorized or malicious access detected during the scope of this potential issue that would have required activation of the CIP-008 Incident Response Plan.

Attachments ()

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

[redacted]se [redacted] users could access the devices going forward. Updates were made to the [redacted] to include a reference to the EMS [redacted] used for password management of the [redacted] devices, going forward. EMS has transitioned shared account password storage and management for [redacted] devices to the EMS [redacted] to automate password changes, as documented in Mitigation Step 4 below. [redacted]

As noted in the originally submitted self-report, the EMS department has completed the following actions to prevent future recurrence: [redacted]

Description of M[redacted]tivities and Completion Dates: [redacted]
1. EMS Compliance[redacted]mployees on the EMS [redacted] process for managing [redacted] passwords and password changes in the [redacted] application. [redacted]
   - Due: 11/16/2016 [redacted]
   - Completed: 11/16/2016
2. EMS changed all shared user account passwords on the [redacted], then [redacted] devices. [redacted]
   - Due: 11/22/2016 [redacted]
   - Completed: 11/22/2016
3. EMS edited the [redacted] to include a reference to the EMS [redacted] used for password management of [redacted] devices going forward using the EMS [redacted].
   - Due: 12/05/2016
   - Completed: 11/30/2016
4. EMS transitioned shared account password storage and management for the [redacted] device[redacted]MS [redacted] applica[redacted]tomate password changes in the event of personnel changes.
   - Due: 12/05/2016 [redacted]
   - Due: 02/17/2017
   - Completed 02/01/2017

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 SERC and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
  - I am [redacted] of [redacted]
  - I am qualified to sign this Mitigation Plan on behalf of [redacted]

- I understand [redacted] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendixe 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 SERC and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

SERC Single Point of Contact (SPOC)

VIEW MITIGATION PLAN CLOSURE: CIP-007-3A (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 2/8/2019

This item was marked ready for signature by [redacted] on 2/8/2019

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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
R5.	SERC2017-402615	SERC2017016832

Date of completion of the Mitigation Plan:

[redacted]

Train users on [redacted]

Milestone Completed (Due: 11/16/2016 and Completed 11/16/2016)
Attachments (0)

[redacted] Compliance [redacted] e EMS [redacted] User Guide p [redacted] naging [redacted] rds and password cha [redacted] e [redacted] application. [redacted]

Change Passwords

Milestone Completed (Due: 11/22/2016 and Completed 11/22/2016)
Attachments (0)

EMS will change all shared user account passwords on the [redacted] current EMS [redacted] devices.

Update EMS Procedures [redacted]

Milestone Completed (Due: 12/5/2016 and Completed 11/30/2016)
Attachments (0)

[redacted] will edit the [redacted] to incl [redacted] rence to the [redacted] User G [redacted] sword management of [redacted] d [redacted] ing forward using the EMS [redacted] application.

Manage Asset Passwords in [redacted]

Milestone Completed (Due: 12/5/2016 and Completed 12/5/2016)
Attachments (0)

[redacted] will transitio [redacted] age an [redacted] ment for the [redacted] ces to t [redacted] application to automa [redacted] rd [redacted] s in the event of personnel cha [redacted]

Submit for Closure [redacted]

Milestone Completed (Due: 2/17/2017 and Completed 2/1/2017)
Attachments (0)

[redacted] Operations [redacted] preher [redacted] w of all requ [redacted] ssocia [redacted] ation plan and prepare [redacted] ry [redacted] packet for SERC review and se [redacted] of this potential violation.

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

Description of Mitigating Activities and Completion Dates:
1. EMS Compliance trained EMS employees on the EMS [redacted] User Guide process for managing [redacted] passwords and password changes in the [redacted] application.
   - Due: 11/16/2016
   - Completed: 11/16/2016
2. EMS changed all shared user account passwords on the [redacted], then current, EMS [redacted] devices.
   - Due: 11/22/2016
   - Completed: 11/22/2016
3. EMS edited the [redacted] to include a reference to the EMS [redacted] User Guide used for password management of [redacted] devices going forward using the EMS [redacted] application.
   - Due: 12/05/2016

- Completed: 11/30/2016

4. EMS transitioned shared account password storage and management for the [redacted] devices to the EMS [redacted] application to automate password changes in the event of personnel changes.
   - Due: 12/05/2016
   - Completed: 12/05/2016

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

5. [redacted] Operations Compliance completed a comprehensive review of all required evidence associated with this mitigation plan and prepared a summary closure packet for SERC review and settlement of this potential violation.
   - Due: 02/17/2017
   - Completed 02/01/2017

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will help prevent future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

Milestone 1

[redacted] This meeting presentation shows (on pages 12-15) that [redacted] Password Change Procedures were covered in the training sessions conducted between 11/10/16 and 11/16/16.

[redacted] These ou look meeting invitations show the times, dates (11/10/16, 11/14/16, 11/15/16, and 11/16/16), and attendees present at EMS training, which covered the process for managing [redacted] passwords in [redacted]

[redacted] This table shows the attendees, and which date of EMS training attended. This training covered the process for managing [redacted] passwords in [redacted]

Milestone 2:

[redacted] This change request shows he date of password changes (5/4/15) for a subset of [redacted]) [redacted] devices.

[redacted] This email shows that at the time the original [redacted] devices were commissioned on or after 5/31/2011, the default manufacturer passwords were to be changed. No additional evidence could be retrieved demonstrating shared account password changes annually after commissioning.

[redacted] This change request shows evidence that all [redacted] current EMS [redacted] [redacted] shared user account passwords were changed as of 11/22/2016. Pages 1-2 list all of the applicable [redacted] devices; Pages 4-6 show password changes conducted by region between 9/23/2016 and 11/22/2016.

[redacted] To determine extent of condition, EMS conducted a review of all EMS shared accounts correlating each with change records demonstrating their annual password change. This document shows the date of last password change for all EMS devices with enabled shared accounts.

Milestone 3:

[redacted] This document is the updated EMS [redacted], which includes, on page 9, a reference to the EMS [redacted] User Guide, which is to be used for password management of [redacted] devices going forward. The change log, describing the edits made on 11/30/2016, is on page 11 of this document.

[redacted] This document is he previous version of the EMS [redacted], dated 6/30/2016.

Milestone 4:

[redacted] This change request shows the enabling of [redacted] for each of the applicable [redacted] [redacted] devices completed as of 12/5/2016 in order to begin performing password management using [redacted]

[redacted] This spreadsheet shows a report exported from [redacted] which demonstrates that the accounts for each of the applicable [redacted] devices have been configured to manage passwords, and also shows the current expiration date (in column E) for each password.

Milestone 5:

[redacted] A comprehensive closure packet containing the files and information referenced above.

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.

Attachment 12

Record documents for the violation of CIP-007-6 R5

12a. The Entities' Self-Report (SERC2017018246)

12b. The Entities' Mitigation Plan designated as SERCMIT014398 submitted July 12, 2018

12c. The Entities' Certification of Mitigation Plan Completion submitted July 12, 2018

12d. The Entities' Self-Report (SERC2018019200)

12e. The Entities' Mitigation Plan designated as SERCMIT014399 submitted July 23, 2018

12f. The Entities' Certification of Mitigation Plan Completion submitted July 23, 2018

12g. The Entities' Self-Report (SERC2017018548)

12h. The Entities' Certification of Mitigation Plan Completion submitted December 6, 2017

12i. The Entities' Self-Report (SERC2016016339)

12j. The Entities' Certification of Mitigation Plan Completion submitted October 26, 2016

VIEW SELF-REPORT: CIP-007-6 R5. (COMPLETED)

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

This item was submitted by [redacted] on 8/24/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:	[redacted]
NERC Registry ID:	[redacted]
JRO ID:	[redacted]
CFR ID:	[redacted]
Entity Contact Information:	[redacted]

REPORTING INFORMATION

Applicable Standard:	[redacted]
Applicable Requirement:	[redacted]
Applicable Sub Requirement(s):	[redacted]
Applicable Functions:	[redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered:	No
Has this Possible Violation previously been reported to other Regions:	No
Date Possible Violation was discovered:	4/21/2017
Beginning Date of Possible Violation:	4/18/2017
End or Expected End Date of Possible Violation:	4/28/2017
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

[redacted], [redacted] Technology Applications Support discovered a potential violation of CIP-007-6 R5.1 while conducting a review of successful and unsuccessful [redacted]ns. It was discovered that [redacted] domain groups [redacted] had been added to the local administrators group on the [redacted] PACS monitoring workstations, thereby providing the potential for allowing electronic access by unauthorized personnel. A review of the domain [redacted] settings by [redacted] Technology Security determined a potential issue where the [redacted] preferences for these assets was failing to properly enforce the domain policies put in place to restrict domain groups to only the [redacted] authorized groups [redacted] Security changed the [redacted] preference ordering on April 24th, 2017 to force a policy refresh on the [redacted] PACS assets, and the domain policy began functioning correctly once the systems were rebooted. Therefore, the root cause of this issue was a failure of [redacted] enforcement of domain rules.

Since the PACS assets ([redacted]) are the only [redacted] CIP assets that reside on the [redacted] domain, an extent of condition review was performed to ensure the same issue was not occurring on the [redacted] PACS servers; it was confirmed as of 04/28/2017 that due to the PACS servers residing within a dedicated [redacted] the domain [redacted] policy issues were not resident on the PACS servers. To prevent future recurrence of this issue, [redacted] will implement similar [redacted] changes for the PACS workstations that are in place for the PACS servers.

On 04/18/2017, one employee, who had authorization for electronic access to the PACS servers, was able to log into the PACS monitoring workstations to check for software issues and update the [redacted] security software. There was an associated change case to perform the same work for the PACS servers, and the employee assumed that the PACS workstations needed the same anti-virus updates as well in accordance with CIP-007-6 R2.
[redacted]
Additionally, while verifying remediation efforts on the above issue, on August 15th, 2017, [redacted] Corporate Services Systems discovered a potential violation of CIP-007-6 R5.1 while conducting a review of successful and unsuccessful authentication attempts on the above mentioned PACS monitoring workstations. It was discovered that an intended limiting [redacted] was being overridden by a higher-level enforced [redacted] control, thus not allowing the lower-level [redacted] control to properly enforce the correct application of the User Right Assignment ([redacted] The User Right Assignment thus contained additional groups which contained users who were not authorized for access on [redacted] PACS monitoring workstations.

The resulting investigation revealed that [redacted] domain groups [redacted] were members of the local [redacted] group on the [redacted] PACS monitoring workstations, thereby providing the potential for electronic non-administrator access by unauthorized personnel. A review of the domain [redacted] settings by [redacted] Technology Security and [redacted] IT [redacted] Infrastructure determined that the governing [redacted] preference control was adding intended group memberships to the [redacted] group, but not removing the existing group memberships, thus not properly enforcing the intended [redacted] group restrictions on the [redacted] PACS workstations. Only one domain group was authorized for PACS workstation access via [redacted]

To remedy this issue, IT Security changed a [redacted] security setting on August 15th, 2017 blocking the application of the higher-level [redacted] thus allowing the intended lower-level [redacted] to contro[redacted] access via the [redacted]' User Right Assignment on the [redacted] PACS assets. Secondly, IT Security changed a [redacted] setting on the [redacted] group membership Group Policy Preference to first remove all existing group members and then add the intended authorized group thus enabling [redacted] access only to authorized users. Therefore, the root cause of this issue was a failure in the application of [redacted]

related controls providing [redacted] enforcement of [redacted] access.

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

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

[redacted] will complete the following:
1) [redacted] Tech Org [redacted] and Security will modify as necessary [redacted] Administrator group policy preferences for the workstations to reapply existing domain controls to enforce removal of errant accounts and allow only the designated / authorized groups. (Completed 4/28/2017)
2) [redacted] Tech Org Applications will implement a more frequent (weekly) review of PACS workstations and servers local administrator accounts until milestone 4 can be implemented. (Completed 07/28/2017)
3) [redacted] Tech Org [redacted] and Security will modify as necessary related security settings on higher level governing [redacted] and update remove existing groups control on [redacted] group policy preferences to reapply the intended governing [redacted] and to enforce the removal of errant accounts to allow only the designated / authorized groups. (Completed 8/15/2017)
4) [redacted] Tech Org [redacted] and Security will implement [redacted] logging and alerting on any group changes to [redacted] settings on PACS workstations. (Complete by 9/25/2017)
5) [redacted] Tech Org [redacted] and Security will realign these PACS workstations on the corporate domain into their own [redacted] to further restrict [redacted] changes. (Complete by 12/22/2017)
6) [redacted] Ops Compliance will prepare a comprehensive closure package of this mitigation plan and submit to SERC. (Complete by 1/15/2018)

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

1/15/2018

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
[redacted]t Logging of PACS [redacted]	9/25/2017	4) [redacted] Tech Org [redacted] and Security will implement [redacted] logging and alerting on any group changes to [redacted] settings on PACS workstations.	No
New PACS [redacted]	12/22/2017	5) [redacted] Tech Org [redacted] and Security will realign hese PACS workstations on the corporate domain into their own [redacted] to further restrict [redacted] changes.	Yes
Closure Package	1/15/2018	6) [redacted] Ops Compliance will prepare a comprehensive closure package.	No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue posed a minimal potential risk and not a moderate or serious risk to the Bulk Power System. The issue represented a potential for unauthorized access to PACS assets by company personnel that had been authorized and granted access in two additional domain groups. In the case of the one system administrator who logged in (causing the issue to be discovered) has worked extensively with CIP assets in the past, has a valid PRA on file, and has completed CIP Security Training annually since 2009. While the System Administrator did not have AMA authorization for electronic access to this particular set of PACS monitoring workstations, she does have AMA au horization for electronic access to the PACS Servers. In the case of the remote desktop access, the individual has AMA access appropriate for he session, and is an authorized user of the PACS asset. The risk was that an unauthorized user might have accessed the PACS workstation. These workstations are designed to provide a minimal build required to use the PACS monitoring software, and are used for CIP-006 monitoring purposes only; they do not provide the ability to add, modify, or delete PSP physical access controls or security configurations.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk, and not a moderate or serious risk to the reliability of the Bulk Power System. The PACS assets ([redacted] applicable to this issue are stripped down [redacted] workstations used by [redacted] /Corporate Security for PSP monitoring of physical access. The PACS application [redacted] on these workstations requires additional layers of authentication before access into the PACS application is possible. Neither the errant domain accounts added in this issue, nor the ability to remotely access these workstations could not have provided access beyond the workstation OS or installed applications. A user accessing the OS without additional assigned application privileges does not have the ability to add, modify, or delete any PSP physical access controls. Additionally, the [redacted] Operators using these workstations have Read-Only access to the PACS application through the use of designated accounts that limit the ability to make PSP/PACS changes. All of the PACS workstations are used and manned in a 24/7 capacity, and have failover redundancy if an issue is experienced on any workstation impacting the [redacted] ability to monitor PSPs. The workstations are configured without Internet facing applications and this limits the impact unauthorized electronic access could have had, both for the two domain accounts errantly added to the local administrator groups, as well as the remote desktop issue identified in this report. The remote desktop issue was discovered during the verification of technical controls put in place to mitigate the original issue. It was addressed immediately, upon discovery.

Additional Comments:

[redacted] C[redacted] Procedures Manual:
[redacted]
Determine if the CIP Cyber System allov[redacted] Interactive User Access (IUA), except in the case of a Medium-Impact BES Cyber System that is not at a Control Center and has no External Routable [redacted] d, determine[redacted] method to enforce authentication for IUA from the following: [redacted]
• Single factor password (for example: User ID and password, PIN). [redacted]
[redacted]n (a combination of tw[redacted] ore of something the user knows (password, PIN), something the use[redacted] as (token), or something the user is (thumbprint). [redacted]
• PSP access (For CIP Cyber Systems that cannot technically or for operational reasons perform IUA, document how all IUA paths, including remote access and local access, are configured f[redacted] suffices for lo[redacted]ation if the person, date, and [redacted]e PSP.) [redacted]

Identify all default or other [redacted]ble on the CI[redacted]ber System which includes vendor supplied default accounts and accounts set up by an operating[redacted]

[redacted] dividual users do not re[redacted]ve authorization to use. Each account must be removed or disabled or renamed where possible. For those accounts that cannot be removed, or disabled, or renamed, the password must be changed. If a password cannot be changed without affecting functionality, document this via vendor manuals or vendor statements. All default or other generic accounts that remain enabled must be documented per section 5.7, Evidence for Each D[redacted]count.

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

[redacted]

The requirements in this section apply to all of the applicable systems and assets defined[redacted]ection 1.2, Scope, as well as their associated Protected Cyber Assets. For all applicable systems and assets (including their associated Protected Cyber Assets), an inventory or list of the enabled Shared User Accounts must be maintained in accordance with[redacted]

1) Approving Access [redacted]

Access requests and approvals for electronic access to a Shared User Account enabled on an applicable system or asset (including any associated Protected Cyber Asset) shall be administered in accordan[redacted]ith the requirem[redacted]b. [redacted]

[redacted]anting Acces[redacted]

Shared User Account credentials shall be issued[redacted]nd maintained in a manner that protects against disclosure of those credentials to any unauthori[redacted]

Shared User Accounts shall only be used to access an applicable system or asset (including any associated Protected Cyber Asset) by Authorized Users approved for access to that Shared User Account within an AMA. Authorized Users of Shared User Accounts are prohibited from disclosing or permitting the use of shared account credentials on an applicable system or asset (including any associated Protected Cyber Assets) by any personnel not approved for access to that Shared User Account within an AMA.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW FORMAL MITIGATION PLAN: CIP-007-6 (REGION REVIEWING MITIGATION PLAN)

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

This item was signed by [redacted] on 7/12/2018

This item was marked ready for signature by [redacted] on 7/11/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-007-6 R5.	SERC2017018246	SERC2017-402822	08/24/2017	Revision Requested	Informal	
CIP-007-6 R5.	SERC2017018246	SERC2017-402822	07/12/2018	Region reviewing Mitigation Plan	Formal	1

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

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

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

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name: [redacted]

Company Address: [redacted]

[redacted]

Compliance Registry ID: [redacted]

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

Name: [redacted]

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

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

Standard: [redacted]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R5.	SERC2017-402822	SERC2017018246	8/24/2017

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

On April 21st, 2017, [redacted] Technolo[redacted]tions Support discovered a potential violation of CIP-007[redacted]R5.1 while cond[redacted] au[redacted]cation atte[redacted]ring works[redacted]ons. It was discovered tha[redacted]) had been added to the local administrators group on the [redacted] PACS monitoring workstations, thereby providing the potential for allowing electronic access by [redacted]authorized personnel. A rev[redacted]of the domain [redacted] settings by [redacted] Technology Security determined a po[redacted]al issue where the [redacted] preferences for these assets was failing to properly enforce the domain policies put in place to restrict domain groups to only the two authorized groups [redacted]rity changed [redacted]cy refresh on [redacted] PACS as [redacted]main [redacted] began funct[redacted]e systems were rebooted. [redacted]

On [redacted]18/2017, or[redacted]horization for electronic acce[redacted] PACS Servers as a system administrator, was [redacted] to log into the PACS monitoring Workstations to check for software issues and update the [redacted] security software. There was an associated change case to perform the same work for the PA[redacted]servers, an[redacted] that the PACS workstations needed the same anti-virus up[redacted] well in accordar[redacted]or [redacted]r authority in adding what she [redacted]lieved to be necessary groups [redacted] to the local administrators group to provide W[redacted]ation administration since she too had authorization for PACS Server access. Howeve[redacted] the [redacted] structure should have prevented her from adding these [redacted] new groups. The [redacted]al dom[redacted] was originally exclusive to administrators who had appropriate authorizations and permissions on the Workstations. Therefore, a failure of [redacted] enforcement of domain rules to prevent the addition of the new domain groups was considered the root cause of the issue, and was further investigated and remediated, as well as discussion and retraining with the PACS server administrators. [redacted]

Since the PACS assets [redacted] CIP assets that reside on the [redacted] domain, an exte[redacted] [redacted] view was performed to ensure the same issue was not occurring on the [redacted] PACS servers; it was confirmed as of 04/28/2017 that due to the PACS servers residing within a dedicated [redacted] domain [redacted] policy issues were not resident on the PACS servers. To pr[redacted]re recurrence of this [redacted]ue, [redacted] has implement similar [redacted] changes for the PACS workstations that were in place for the PACS servers. [redacted]

Additionally, w[redacted]ifying remediation efforts on t[redacted]e issue, on August 15th, 2017, [redacted] Corp[redacted]es Systems dis[redacted]red a potential violation of CIP-007-6 R5.1 while conducting a review of successful and unsuccessful authentication attempts on the above mentioned PACS monitoring workstations. It was discovered that an

intended limiting control was being overridden by a higher-level enforced control, thus not allowing the lower-level control to properly enforce the correct application of the The thus contained a ed users who were not authorized for electronic access to the PACS monitoring workstations.

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

The resulting investigation revealed that domain groups were members of the local group on the PACS monitoring workstations, thereby providing the potential for electronic non-administrator access by unauthorized personnel. A review of the domain settings by Technology Security and IT determined that the governing preference control was adding intended group memberships to the group, but not removing the existing group memberships, thus not properly enforcing the intended group restrictions on the PACS workstations. Only one domain group was authorized for PACS workstation access via

The root cause of this issue was due to a system administrator misunderstanding the way in which group policy is applied to systems and the appropriate layering of controls. Through the course of resolving the issue, the systems administrator support group personnel have met with support to ensure a more thorough understanding of the way in which policy is applied and more specifically, how to limit a "higher level" (more broad) policy from superseding a lower level (more specific) policy.

To remedy this issue, IT Security changed a security setting on August 15th, 2017 blocking the application of the higher-level thus allowing the intended lower level to control access via the on the PACS assets. Secondly, IT Security changed a setting on the group membership Group Policy Preference to first remove all existing group members and then add the intended authorized group thus enabling access only to authorized users. Therefore, the root cause of this issue was a failure in the application of two related controls providing enforcement of Remote Desktop User access.

There was no known harm that occurred as a result of these issues.

Attachments ()

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

This issue involved a Techno ations Support PACS administrator who discovered that domain groups ha n added t group on PACS monitoring worksta y unauthorized personnel. This issue was discovered w le conducting an internal review of successful and unsuccessful authentication attempts on the PACS monitoring wo ations. Addition tion efforts o e above issue, on August 15th, 2017, Corporate Services tems discovered a potential violation of CIP-007-6 R5.1 while conducting a review of successful and unsuccessful authentication attempts on the above m The main groups) were memb the local group on th workstations, thereby providing the potential for electronic n inistrator access by unauthorized personnel.

Th rpose of th to allow system administrato ed access to server operating systems and so e to maintain baseline configurations, perform security patching, and software up h sets across the corporate domain. Administrator groups are separated based on the su matter exp r as well as their specific job responsibilities. The administr e first instance d the potential to access the PACS monitoring workstation access controls at PSPs protecting High and M n Impact BES Cyber Systems at Control Centers and Transmission Substations. The PA kstations used by Security Monitoring Operators are locate secured PSPs at sites o Security personnel. The electronic access permitted via these two groups was limited to the Operating System and non-PACS software only ese PACS workstations, and did not allow electronic access to the PACS application software on these workstations (i.e., could not have allowed access or changes to PACS physical access controls or configurations – they could have only impacted access to the monitoring workstations themselves).

As for the second instar a subset of domain users ha y note desktop cli PACS monitoring workstations remotely. This issue involves the same CS monitoring workstation assets associated with the monitoring of physical access controls at PSPs pr mpact B yber Systems at Control Centers and Transmission Substa y attempted access b quired knowledge of th pecific PACS monitoring workstation host name(s) and those personnel must be a of the used for authentication to the workstations. This reduces the potential for exposure from approximately employees to approximately users across the system with a orate Again, this wo ave only granted the potential to log in to the workstations at the OS level, and would not have allowed access to the PACS application software on those workstations (i.e., no ability to monitor or change PSP physical access ols in place at all PSPs).

Once on the workstation, additional layers of authentication re required before access into the PACS application is possible. In both instances, due to layered electronic access controls, the number of people who were actually able to access the PACS application never changed - i.e. all users that could have accessed the PACS application had appropriate authorization for access. Any unintended loss of a PACS monitoring workstation is mitigated by the fact that there are multiple monitoring workstations at each site (primary and backup), and the loss would not have impacted the ability to maintain physical access controls, monitoring controls, or logging controls at each PSP.

As part of remediation and mitigation of this issue, the PACS administrator refined system alerting to cover monitoring the domain groups for unauthorized additions (Milestone #4). The second issue was discovered while performing testing on the implementation of Milestone #3, where the Technology Organization modified the to force them to apply in the intended order, thereby consistently enforcing the appropriate electronic access controls.

As part of the CIP Procedures Manual has implemented the to address CIP-007-6 R5.1.
This procedure takes all of the various requirements and tasks associated with the technical management of cyber assets or cyber systems (CIP-007 and the baseline configuration and vulnerability assessment portions of CIP-010) and organizes these tasks by the lifecycle stage of the applicable system for ease of use by support personnel.
It includes the steps to follow for planning for a new CIP Cyber System (Section 4.1), commissioning a new CIP Cyber Systems (Section 4.2), maintaining existing CIP Cyber Systems including tasks performed at varying periodicity throughout the system's lifetime (Section 4.3), and decommissioning CIP Cyber Systems (Section 4.4).
Requirement 5 Part 5.1 is addressed in the procedure as follows:
• Planning for New CIP Cyber Systems - Section 4.1, Step 9 requires the assessment of whether interactive user access is allowed and outlines the three methods allowed for authentication and the requirement to file for a TFE if the listed methods are not feasible. The following three methods are acceptable:
o Single Factor Password
o Multiple Factor Authentication
o PSP Access (i.e. Local Access)
• Commissioning CIP Cyber Systems - Section 4.2, Step 13 requires the implementation and configuration of the method chosen in Section 4.1.

As part of the CIP Procedures Manual, has implemented the , CIP-004-6 R4. states:
The requirements in this section apply to all of the applicable systems and assets defined in Section 1.2, Scope, as well as their associated Protected Cyber Assets.

For all applicable systems and assets (including their associated Protected Cyber Assets), an inventory or list of the enabled Shared User Accounts must be maintained in accordance with
1) Approving Access
• Access requests and approvals for electronic access to a Shared User Account enabled on an applicable system or asset (including any associated Protected Cyber Asset) shall be administered in accordance with the requirements of Section 4.2, Subsection 2) Approving Access, Items a & b.

2) Granting Access
• Shared User Account credentials shall be issued to Authorized Users and maintained in a manner that protects against disclosure of those credentials to any unauthorized personnel.
• Shared User Accounts shall only be used to access an applicable system or asset (including any associated Protected Cyber Asset) by Authorized Users approved for access to that Shared User Account within an AMA. Authorized Users of Shared User Accounts are prohibited from disclosing or permitting the use of shared account credentials on an applicable system or asset (including any associated Protected Cyber Assets) by any personnel not approved for access to that Shared User Account within an AMA.

This issue was not discovered through a formal internal controls process; however, the PACS administrator was already set up to receive real-time alerts from the logging servers regarding login events as part of his CIP 007-6 R4 and CIP-007-6 R5.1 work duties for the PACS systems. Activity in the logs is confirmed to be associated with authorized users, and any logs that are not are investigated. The PACS administrator was reviewing server logs when he detected that another sysadmin in the Technology Organization administrator group logged in on a workstation. This sysadmin logged in to update the antivirus definitions. The PACS administrator

investigated the login and this is when he discovered the changes to the local administrator group. He performs this internal control watchdog activity and log review as part of his normal daily administration duties, and this has been in place since 7/1/2016.

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

Attachments ()

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

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

Description of Mitiga[redacted]tivities: [redacted] will complete the following: [redacted]
1) [redacted] Tech Org [redacted] and Secu[redacted]y will modify as necessary [redacted]r the workstations to reapply existing domain controls to e[redacted]rce removal of errant accounts and allow only the designated / authorized groups. (Completed 4/[redacted]2017)
2) [redacted] Tech Org App [redacted] ore frequen [redacted] ekly) review of PACS workstations a[redacted]rvers local adminis[redacted]r accounts until milestone 4 can be implemented. (Completed 07/28/2017) [redacted]
3[redacted] and Security [redacted]el governing [redacted] and updat[redacted]g [redacted]s control on [redacted] group policy preferences to reapply the intended governing [redacted] and to enforce the removal of errant accounts to allow only the designated / authorized groups. (Completed 8/15/2017)
4) [redacted] Tech Org [redacted] and Security will implement [redacted] logging and alerting on any group changes to [redacted] settings on PACS workstations. (Completed 9/21/2017) [redacted]
5) [redacted] Tech Org [redacted] and Security will realign these PACS workstations on the [redacted] domain into the [redacted] changes. (Completed 12/13/[redacted]17) [redacted]
6) [redacted] Ops Compliance will prepare a comprehensive closure package of this mitigation p[redacted] an [redacted] (Completed 1/11/2018) [redacted]
Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones wil[redacted]vent future recurrence of this issue.

Regarding the extent of condition performed, it covered a review of the PACS assets that are used to provide physical security protections for our [redacted] high and medium impact BES Cyber Systems and associated EACMS and PCAs. We feel that the possibility of the same issues occurring outside of the PACS assets is minimal based on the use of ded[redacted] the PACS assets are the only [redacted]at reside on the [redacted] domain. Due to the domain structuring, the restructuring of the domain [redacted] separate Organizational Unit for PACS systems isolates the PACS workstations from changes that occur to [redacted] Domain [redacted]hings like patch management and AV signature roll-outs to [redacted] domain groups like [redacted] [redacted]ures in a timely manner [redacted]rease the security posture of those assets, the lack of close coordination between [redacted] supp[redacted] group ha[redacted] instances where changes were not fully coordinated at the time they were made to ensure all checks were [redacted] and all documentation upda[redacted]e completed in the required time[redacted]es. [redacted] mitigation, the [redacted] Technology Organization has greatly reduced the likelihood of this issue recurring by placing these PACS assets in a revised Organizational Unit wi h very restrictive polices. Tech Org EACMS assets are already in anothe[redacted]icated NERC CIP environment and were segmented int[redacted] dedicated environment based on risk an[redacted]s. Our Energy Management System resides in its own [redacted] reside[redacted]ot subject to any [redacted]

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:

1/15/2018

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

[redacted] Logging of PACS [redacted]

Milestone Completed (Due: 9/25/2017 and Completed 9/21/2017)

4) [redacted] Tech Org [redacted] and Security will implement [redacted] logging and alerting on any group changes to [redacted] settings on PACS workstations.

New PACS [redacted]

Milestone Completed (Due: 12/22/2017 and Completed 12/13/2017)

5) [redacted] Tech Org [redacted] and Security will realign these PACS workstations on the corporate domain into their own [redacted] to further restrict [redacted] changes.

Closure Package [redacted]

Milestone Completed (Due: 1/15/2018 and Completed 1/11/2018)

6) [redacted] Ops Com [redacted]mprehensive closure packag[redacted] [redacted]

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):

(i) There are no known additional risks or impacts to the BPS while the actions in this mitigation plan are being completed.
(ii) [redacted] does not plan to implement additional actions that would increase risks to the reliability of the BPS as part of this mitigation plan.

[redacted] assesses this issue posed a minimal actual risk, and not a serious or substantial risk to the reliability of the bulk electric system. The PACS assets (monitoring workstations) applicable to this issue are stripped down [redacted] workstations used by [redacted] Corporate Security for PSP monitoring of physical access. The PACS applicatior [redacted] on these workstations requires additional layers of authentication before access into the PACS application is possible. Neither the errant domain accounts added in this issue, nor the ability to remotely access these workstations could not have provided access beyond the workstation [redacted] or installed applications. A user accessing the [redacted] without additional assigned application privileges does not have the ability to add, modify, or delete any PSP physical access controls. Additionally, the [redacted] Operators using these workstations have Read-Only access to the PACS application through the use of designated accounts that limit the ability to make PSP/PACS changes. All of the PACS workstations are used and manned in a 24/7 capacity, and have failover redundancy if an issue is experienced on any workstation impacting the [redacted] ability to monitor PSPs. The workstations are configured without Internet facing applications and this limits the impact unauthorized electronic
access could have had, both for the [redacted] domain accounts errantly added to the local administrator groups, as well as the remote desktop issue identified in this report. The remote desktop issue was discovered during the verification of technical controls put in place to mitigate the original issue, and was addressed immediately upon discovery.
For the mitigation of the subsequently found issue involving the layering of Active Directory controls (blocking the higher-level controls), there was risk associated with rearranging the order in which the application of Active Directory controls was applied since the changes had to be implemented in the [redacted] Active Directory. Any problems encountered in those changes had the potential to adversely impact [redacted] or more users, so additional time for testing the changes was

warranted with this mitigation step, which was completed 8/15/2017. This mitigation step was implemented without negative impact. The remaining Milestone #6 to separate these systems into their own organizational unit (OU) will additionally reduce risk going forward.

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 Mitiga ion 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 will minimize the probability of future violations of the same requirements by realigning these PACS workstations on the [redacted] domain into their own Organizational Unit to further restric[redacted] changes.
As noted in the originally submitted self-report, [redacted] Tech Org has completed the following actions to prevent future recurrence:
1) [redacted] Tech Org [redacted] and Security will modify as necessary [redacted] Administrator group policy preferences for the workstations to reapply existing domain controls to enforce removal of errant accounts and allow only the designated / authorized groups. (Completed 4/28/2017)
3) [redacted] Tech Org [redacted] and Security will modify as necessary related security settings on higher level governing [redacted] and update or remove existing groups control on [redacted] group policy preferences to reapply the intended governing [redacted] and to enforce the removal of errant accounts to allow only the designated / authorized groups. (Completed 8/15/2017)
4) [redacted] Tech Org [redacted] and Security will implement [redacted] logging and alerting on any group changes to [redacted] settings on PACS workstations. (Complete by 9/25/2017)
5) [redacted] Tech Org [redacted] and Security will realign these PACS workstations on the corporate domain into their own [redacted] to further restrict [redacted] changes. (Complete by 12/22/2017)

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 SERC and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
  - I am [redacted] of [redacted]
  - I am qualified to sign this Mitigation Plan on behalf of [redacted]
  - I understand [redacted] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendixe 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 SERC and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

SERC Single Point of Contact (SPOC)

VIEW MITIGATION PLAN CLOSURE: CIP-007-6 (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 7/12/2018

This item was marked ready for signature by [redacted] on 7/11/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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
R5.	SERC2017-402822	SERC2017018246

Date of completion of the Mitigation Plan:

[redacted]

[redacted]t Logging of PACS[redacted]

Milestone Completed (Due: 9/25/2017 and Completed 9/21/2017)
Attachments (0)

4)[redacted] Tech Org [redacted] and Security will implement [redacted] logging and alerting on any group changes to [redacted] settings on PACS workstations.

New PACS [redacted]

Milestone Completed (Due: 12/22/2017 and Completed 12/13/2017)
Attachments (0)

5)[redacted] Tech Org [redacted] and Security will realign these PACS workstations on the [redacted] domain into their own [redacted] to further restrict [redacted] changes.

Closure Package [redacted]

Milestone Completed (Due: 1/15/2018 and Completed 1/11/2018)
Attachments (0)

6)[redacted] Ops Com [redacted] nprehensive closure packag [redacted] [redacted]

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

Description of Mi[redacted] Activities: [redacted] will complete the following:
1)[redacted] Tech Org [redacted] and Security will modify as necessary [redacted] Administrator group policy preferences for the workstations to reapply existing domain controls to enforce removal of errant accounts and allow only the designated / authorized groups. (Completed 4/28/2017)
[redacted] review of PACS workstations and servers local administrator accounts until milestone 4 can be implemented. (Completed 07/28/2017)
[redacted] odify as necessary related security settings on higher level governing [redacted] and update remove existing groups control on [redacted] group policy preferences to reapply the intended governing [redacted] and to enforce the removal of errant accounts to allow only [redacted]
4)[redacted] Tech Org [redacted] and Security will implement [redacted] logging and alerting on any group changes to [redacted] settings on PACS workstations. [redacted]
5)[redacted] Tech Org [redacted] and Security will realign these PACS workstations on the corporate domain into their own [redacted] to further [redacted]
6)[redacted] Ops Compliance will prepare a comprehensive closure package of this mitigation plan and submit to [redacted]. (Completed 1/11/2018) [redacted]
Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

[redacted] sets that are used to provide physical security protections for our [redacted] high and medium impact BES Cyber Systems and associated EACMS and PCAs. We feel that the possibility of the same issues occurring outside of the PACS assets is minimal based on the use of dedicated domains for CIP assets ([redacted]), whereas the PACS assets are the only in-scope CIP assets that reside on the [redacted] turing of the domain into a separate Org [redacted] al Unit for PACS systems isolates the PACS workstations from changes that occur to the [redacted] Domain for things like patch management and AV signature roll-outs to corporate domain groups [redacted] se the security posture of t [redacted] sets, the lack [redacted] rdination [redacted] grou [redacted] where change [redacted] rdinated at the time they were made [redacted] de and all documentation updates were com [redacted] ed timeframes. Hence, as a mitigation, the [redacted] Technology Organization has greatly reduced the likelihood of this issue recurring by placing these PACS assets in a revised Organizational Unit with very restrictive polices. Tech Org EACMS assets are already in another dedicated NERC CIP environment and were segmented into this dedicated environment based on risk analysis. Our Energy Management System resides in its own separate domain and the [redacted] based assets in Substations reside in their own domain, not subject to any [redacted] applied to [redacted]

Description of the information provided to SERC for their evaluation *

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

Closure Packet:
MS1:
Demonstrates removal of errant accounts and allows only the designated / authorized groups.
MS2:
Shows evidence of weekly review of policy domain groups to AMA Gra r he PACS systems for PACS servers.
Shows evidence of weekly review of policy domain groups to AMA Grants for he PACS systems for PA servers.
Shows evidence of weekly review of policy domain groups to AMA Grants for the PACS systems for PA workstation
Shows evidence of weekly review of policy domain groups to AMA Grants for the PACS systems for PA workstations.
Shows evidence of weekly review of policy domain groups to AMA Grants for the PACS systems for PACS workstations.
MS3:
shows implementation of group policy changes required to fix th ue discovered during the testing of changes required for Milestone #4.
MS4:
shows samples from live testing of the alerting implemented in Milestone #4.
MS5:
shows realignment of the workstations
n the to a dedicated structure governed by dedicated objects that are singularly linked to this new structure, creating the restrictive alignment d ed.

MS6:
This comprehensive closure packet

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.

VIEW SELF-REPORT: CIP-007-6 R5. (COMPLETED)

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

This item was submitted by [redacted] on 2/16/2018

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [redacted]

NERC Registry ID: [redacted]

JRO ID: [redacted]

CFR ID: [redacted]

Entity Contact Information: [redacted]

REPORTING INFORMATION

Applicable Standard: [redacted]

Applicable Requirement: [redacted]

Applicable Sub Requirement(s): [redacted]

Applicable Functions: [redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

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

Date Possible Violation was discovered: 12/18/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 1/8/2018

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On 12/18/2017, the [redacted] Technology Organization (Tech Org) group discovered a possible CIP-007-6 R5.4 issue where (2) EACMS' commissioned on 7/1/2016 did not have the default account password for the [redacted] application account changed prior to the commissioning of the devices. This issue was discovered during a pre-security controls check to upgrade the [redacted] software. Upon discovery on 12/18/2017, the default account password on the [redacted] servers [redacted] was changed on 12/20/2017. Due to a documentation error, the default account password change checklist incorrectly noted a password change had been completed and the account type was categorized as a [redacted] The account is a pre-installed application user account provided by the vendor. Therefore, the scope of non-compliance is approximately 17 months and 19 days.

As part of a review for those systems which utilize the [redacted] application account, on 1/5/2018, it was discovered [redacted] additional EACMS' commissioned on 7/1/2016 did not have the default account password for the [redacted] account changed prior to the commissioning of the device. In addition, it was discovered the [redacted] account was not identified and inventoried for these [redacted] assets in accordance with CIP-007-6 R5.2. Upon discovery, the default account password on the [redacted] servers [redacted] was changed on 01/08/2018. The CIP-007-6 R5.2 account inventory documentation was updated on 01/08/2018. The scope of non-compliance is approximately 18 months and 7 days. The [redacted] servers associated with this issue are classified as EACMS associated with Medium Impact Transmission Substation BES Cyber Systems, and are used in the log monitoring and alerting processes for CIP-007-6 R4.

The root cause of this issue was a complete account inventory was not performed when these servers came into scope of CIP V5 on 7/1/2016. [redacted] Tech Org personnel failed to follow the [redacted] CIP Policy and Procedures Manual, [redacted] procedure and the [redacted] for these [redacted] EACMS assets. At the time the [redacted] account was inventoried and categorized, field personnel did not categorize the account accurately as a default account provided by the vendor, and did not change the default password. Both the procedure and the business unit-specific work practice outline the inventory, identification, change and validation process for default account passwords upon commissioning of new in-scope CIP cyber assets, and this is considered an issue specific to the management of these [redacted] assets and not a pervasive issue across [redacted] Tech Org-managed CIP EACMS assets.

To mitigate this issue, the passwords were changed and the documentation was updated to achieve compliance with CIP-007-6 R5.2 and R5.4. Tech Org added additional instruction to the [redacted] work practice to provide more specifics for account identifica ion, and a flowchart detailing steps to be performed for CIP-007-5 R5 account management and password changes. An extent-of-condition review will be performed on all [redacted] Tech Org managed assets to confirm there are no addi ional enabled device accounts that were not properly identified in the inventory (R5.2) and there are no other default passwords that were not changed upon commissioning (R5.4) on 7/1/2016, including any devices commissioned thereafter. Additionally, to prevent future recurrence of this issue, [redacted] Tech Org leadership will conduct reinforcement counselling with personnel responsible for account management of [redacted] Tech Org managed CIP assets.

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

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

If Yes, Provide description of Mitiga ing Activities:

1) [redacted] Tech Org will change the [redacted] default password on the [redacted] devices [redacted]. Complete 12/20/2017
2) [redacted] Tech Org, Risk and Compliance Analyst will conduct a review session with the [redacted] Tech Org personnel responsible for changing the [redacted] account password and the importance of compliance with the CIP Program. Complete 1/2/2018
3) [redacted] Tech Org will change the [redacted] default password on the [redacted] devices [redacted]. Complete 1/8/2018
4) [redacted] Tech Org will update the CIP-007 R5.2 documentation for the [redacted] servers and the [redacted] Servers. Complete 1/8/2018
5) [redacted] Tech Org will modify the [redacted] work practice to provide more specific instruction for account identification and password change requirements. Complete 2/8/2018
6) [redacted] Tech Org leadership will conduct reinforcement counselling with personnel responsible for account management of [redacted] Tech Org managed CIP assets. Due 4/5/2018
7) [redacted] Tech Org will perform a review of all [redacted] Tech Org-managed CIP Cyber Systems and associated CIP-007 R5 documentation to ensure all accounts are identified, inventoried, and meet the CIP-007 R5.2, R5.3, and R5.4 requirements. Due 5/4/2018
8) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Due 5/30/2018

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

5/30/2018

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Training	4/5/2018	6) [redacted] Tech Org leadership will conduct reinforcement counselling with personnel responsible for account management of [redacted] Tech Org managed CIP assets.	Yes
CIP BES Cyber System Review	5/4/2018	7) [redacted] Tech Org will perform a review of all [redacted] Tech Org-managed CIP Cyber Systems and associated CIP-007 R5 documentation to ensure all accounts are identified, inventoried, and meet the CIP-007 R5.2, R5.3, and R5.4 requirements.	No
Closure Package	5/30/2018	8) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.	No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue posed a minimal potential risk, and not a serious or substantial risk to the reliability of the bulk electric system. Potential risk could include application access by an unauthorized user with access to or knowledge of vendor default account passwords. An actor with malicious intent could have potentially rendered one or more of these [redacted] servers inoperable or unavailable, when needed. This could have also provided the ability for the introduction of malicious code or configuration changes that made these devices susceptible to exploitation. The root cause of this issue was a failure identify and categorize the [redacted] application account. Tech Org personnel failed to thoroughly follow new BES Cyber Asset commissioning steps to document and change default account passwords for existing devices that came into scope of new CIP V5 requirements on 7/1/2016. The [redacted] servers are physically protected within a PSP, and the other logical protections required by the CIP standards were in place to further minimize the actual possibility of unauthorized access or the introduction of malicious code on these devices.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk, and not a serious or substantial risk to the reliability of the bulk electric system. [redacted] Tech Org's failure to properly follow proper default account inventory and password change procedures could have allowed access by an unauthorized user with access to or knowledge of vendor default account passwords. An actor with malicious intent could have potentially rendered one or more of these [redacted] servers inoperable or unavailable. [redacted] This is considered an issue specific to the management of these [redacted] assets and not a pervasive issue across [redacted] Tech Org-managed CIP EACMS assets. The scope of non-compliance occurred on [redacted] out of [redacted] devices managed by the [redacted] Tech Org.

Additional Comments:

[redacted] Transmission has the following policies, plans, procedures, and business unit work practices to address CIP-007-6 R5:

[redacted]
• CIP-007-6 R5.2 and CIP-007-6 R5.4
• Section 4.1 (Planning for a NEW Cyber System), Section 4.1.8, (Baseline Configuration), Step 10
10. Identify all default or other generic accounts available on the CIP Cyber System which includes vendor supplied default accounts and accounts set up by an operating system or application to perform specific operations that individual users do not receive authorization to use. Each account must be removed or disabled or renamed where possible. For those accounts that cannot be removed, or disabled, the password must be changed. If a password cannot be changed without affecting functionality, document this via vendor manuals or vendor statements. All default or other generic accounts that remain enabled must be documented per section 5.7, Evidence for Each Default or Generic Account.
• Section 4.2, Commission CIP Cyber Systems, Step 14
14. Change all known default passwords and validate that the passwords have been changed.

[redacted]
• Section 4.1 Typical Account Types and Definitions, Step 7
Default and other generic accounts provided by a vendor, [redacted] should have the ID Disabled, ID Removed, ID Renamed, or Password Changed prior to production use of the Cyber Asset or BES Cyber System.

• Section 4.1.1 Default or Generic Accounts Listing and Changing Known Default Passwords
Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). Using the above template, document all of the Default or Generic Accounts.

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

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW FORMAL MITIGATION PLAN: CIP-007-6 (REGION REVIEWING MITIGATION PLAN)

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

This item was signed by [redacted] on 7/23/2018

This item was marked ready for signature by [redacted] on 7/23/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-007-6 R5.	SERC2018019200	SERC2018-402985	02/16/2018	Revision Requested	Informal	
CIP-007-6 R5.	SERC2018019200	SERC2018-402985	07/23/2018	Region reviewing Mitigation Plan	Formal	1

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

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

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

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name: [redacted]

Company Address: [redacted]

[redacted]

Compliance Registry ID: [redacted]

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

Name: [redacted]

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

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

Standard: [redacted]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R5.	SERC2018-402985	SERC2018019200	2/16/2018

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

On 12/18/2017, the [redacted] Org) group discovered a p[redacted]le CIP-007-6 R5.4 issue where [redacted] EACMS' commissioned on 7/1/2016 did not have the default account password for the [redacted] application account changed prior to the commissioning of the devices. This issue was discovered during a pre-security controls check to upgrade the [redacted] software as par[redacted] CIP-010-2 R1. Upon discovery on 1[redacted]7, the [redacted] servers [redacted] was changed on 12/20/2017. Due to a documentation error, the default account password change checklist incorrectly noted a password change had been completed and the account type was categorized as a [redacted] The [redacted] preinstalled application use[redacted] [redacted]dor. Therefore, th[redacted]cope o[redacted]o[redacted]nately 17 months and 19 days.

As part of a review for those systems which utilize the [redacted] application account, on 1/5/2018, it was discovered [redacted] additional EACMS' commissioned on 7/1/2016 did not h[redacted] the default account password for the [redacted] account [redacted]ged prior to the commissioning of the device. In addition, it was discovered the [redacted] account was not identified and inventoried for these [redacted] assets in accordance with CIP-007-6 R5.2. Upon discovery, the default account password on the [redacted] servers [redacted] was changed on 01/08/2018. The CIP-007-6 R5.2 account inventory documentation was updated on 01/08/2018. The scope of non-compliance is approximately 18 months and 7 days. The [redacted] servers associated with this issue are classified as EACMS associated with Medium Impact Transmission Substation BES Cyber Systems, and are used in the log monitoring and alerting processes for CIP-007-6 R4. [redacted]

The root cause of th[redacted] issue was a complete account inventory was not performed when these servers came into scope of CIP V5 on 7/1/2016. [redacted] Tech Org personnel failed to follow the [redacted] CIP Policy and Procedures Manual, [redacted] procedure and the [redacted] for these [redacted] EACMS assets. At the time the [redacted] account was inventoried and categorized, personnel did not categorize th[redacted]curately as a default account provided by the vend[redacted]r [redacted]not change the [redacted]ific work [redacted]nventory, identification, change and valid[redacted]ocess for default account passwo[redacted]pon commissioning of new in-scope CIP [redacted]ssets, and this is considered an issue specific to the management of these [redacted] assets.

To mitigate this issue, the passwords were changed and the do[redacted]ation was updated to achieve compliance with CIP-007-6 R5.2 and R5.4. [redacted]ent-of-condition re[redacted] completed as part of milestone 7 of this mitigation plan on 5/3/2018, was performed on all [redacted] Tech Org managed assets to confirm there are no additional enabled device accounts that were not properly identified in the inventory (R5.2) and there are no other default passwords that were not changed upon [redacted]g (R5.4) on 7/1/2016, including any devices commissioned thereafter.

A lack of oversight or training in the Tech Org may have led to individuals not following the procedure and work practice. To prevent future recurrence of this issue, as part [redacted] to provide more specific instructions for account identification, and a flowchart detailing steps to be performed for CIP [redacted] changes. Additionally, [redacted] Tech Org leadership conducted reinforcement counselling with personnel responsible for account management of [redacted] Tech Org managed CIP assets as part of milestone 6 completed on 3/12/2018.

There was no known harm that occurred as a result of this issue.

Attachments ()

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

This issue involved [redacted] servers managed by the [redacted] Technology Organization that are in place for the operating company Transmission Substations organizations to comply with CIP [redacted] rity Event Monitoring. The servers are classified as EACMS associated with and used for log monitoring and alerting of medium impact Transmission [redacted] ber Systems in [redacted] medium impact Substations across [redacted]

[redacted] servers are located at the [redacted] data center and [redacted] at the [redacted] data center, physically protected within PSPs and with other logical protections in place as required by the CIP standards to further minimize the possibility of unauthorized logical access.

On 5/3/2018, the [redacted] Technology Organization (Tech Org) c[redacted] view of al[redacted] Tech Org-managed CIP Cyber Systems and associated CIP-007 R5 [redacted] ensure all accounts are identified, inventoried, and [redacted] eet the CIP-007 R5.2, R5.3, and R5.4 requirements. The review was completed as part of the self-[redacted] tion plan [redacted] llowing is a description of additional findings documented in the review:

PACS Workstations

- [redacted] Shared account was available on [redacted] PACS Workstations, and the account was not documented in the account inventory. The [redacted] account was deleted from these [redacted] PACS workstations on 4/17/2018.
- [redacted] domain account had administrative rights on the [redacted] host systems [redacted] and the account was not recorded in the [redacted] Default Accounts listing for these [redacted] hosts. The accounts were added to the [redacted] Default Accounts listing as part of this review mitigation.
- [redacted] account [redacted] on the [redacted] hosts [redacted] had administrative rights to host configuration information when accessing the hosts via the [redacted] interface. This account was not recorded in the Default Accounts listing for these [redacted] hosts. The [redacted] interfaces for the [redacted] Hosts have been disconnected from the network.

[redacted]

It was determined the following accounts were not initially documented in the [redacted] Default Accounts listing. The [redacted] Default Accounts listing was updated on 4/17/2018 to include:

[redacted]

[redacted] Logger

It was determined the following accounts were not initially documented in the [redacted] Default Accounts listing. The [redacted] Default Accounts listing was updated on 4/17/2018 to include:

[redacted]

Compromise of these EACMS servers via a vulnerability associated with the presence of default passwords for the [redacted] or other discovered accounts could have impacted the ability to perform security event monitoring of Substation BCAs and PCAs. However, this would not have had a direct impact on the BES or the BCAs/PCAs contained within the [redacted] Substations.

The [redacted] Technology Organization manages [redacted] EACMS servers/appliances (domain controllers, intermediate systems, [redacted] appliances, [redacted] servers, [redacted] servers, and ESP firewall management consoles/servers), [redacted] PACS servers, [redacted] PACS monitoring workstations, [redacted] PACS controller panels, and [redacted] dedicated TCA laptops.

As part of the [redacted] CIP Procedures Manual, [redacted] has implemented the [redacted] to address CIP-007-6 R5. [redacted] addresses the lifecycle of applicable CIP Cyber Systems. This procedure takes the various requirements associated with the technical management of cyber assets or cyber systems (including the system access control requirements of CIP-007-6 R5.2 and R5.4) and organizes these tasks by the lifecycle stage of the applicable system for ease of use by support personnel. It includes the steps to follow for planning for a new CIP Cyber System (Section 4.1), commissioning a new CIP Cyber Systems (Section 4.2), maintaining existing CIP Cyber Systems including tasks performed at varying periodicity throughout the system's lifetime (Section 4.3), and decommissioning CIP Cyber Systems (Section 4.4).

- Section 4.1 (Planning for a NEW Cyber System), Section 4.1.8, (Baseline Configuration), Step 10

10. Identify all default or other generic accounts available on the CIP Cyber System which includes vendor supplied default accounts and accounts set up by an operating system or application to perform specific operations that individual users do not receive authorization to use. Each account must be removed or disabled or renamed where possible. For those accounts that cannot be removed, or disabled, the password must be changed. If a password cannot be changed without affecting functionality, document this via vendor manuals or vendor statements. All default or other generic accounts that remain enabled must be documented per section 5.7, Evidence for Each Default or Generic Account.

- Section 4.2, Commission CIP Cyber Systems, Step 14

14. Change all known default passwords and validate that the passwords have been changed.

The [redacted] Technology Organization [redacted] also maintains the following [redacted] which dictates the necessary steps to address compliance with CIP-007-6 R5:

- Section 4.1 Typical Account Types and Definitions, Step 7

Default and other generic accounts provided by a vendor, per [redacted] should have the ID Disabled, ID Removed, ID Renamed, or Password Changed prior to production use of the Cyber Asset or BES Cyber System.

- Section 4.1.1 Default or Generic Accounts Listing and Changing Known Default Passwords

Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). Using the above template, document all of the Default or Generic Accounts.

This issue was not discovered through a formal internal controls process; however, the issue was discovered through execution of documented processes established to comply with CIP-010-2 R1.

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:

Description of Mitigating Activities:

1) [redacted] Tech Org will change the [redacted] default password on the [redacted] devices [redacted]. Complete 12/20/2017
2) [redacted] Tech Org, Risk and Compliance Analyst will conduct a review session with the [redacted] Tech Org personnel responsible for changing the [redacted] account password and the importance of compliance with the CIP Program. Complete 1/2/2018
3) [redacted] Tech Org will change the [redacted] default password on the [redacted] devices [redacted]. Complete 1/8/2018
4) [redacted] Tech Org will update the CIP-007 R5.2 documentation for the [redacted] servers and the [redacted] Servers. Complete 1/8/2018
5) [redacted] Tech Org will modify the [redacted] work practice to provide more specific instruction for account identification and

password change requirements. Complete 2/8/2018
6) [redacted] Tech Org leadership will conduct reinforcement counselling with personnel responsible for account management of [redacted] Tech Org managed CIP assets. Due 4/5/2018 Completed 3/12/2018
7) [redacted] Tech Org will perform a review of all [redacted] Tech Org-managed CIP Cyber Systems and associated CIP-007 R5 documentation to ensure all accounts are identified, inventoried, and meet the CIP-007 R5.2, R5.3, and R5.4 requirements. Due 5/4/2018 Completed 5/3/2018
8) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Due 5/30/2018 Completed 5/18/2018

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

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

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:

5/30/2018

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

Training

Milestone Completed (Due: 4/5/2018 and Completed 3/12/2018)

6) [redacted] Tech Org leadership will conduct reinforcement counselling with personnel responsible for account management of [redacted] Tech Org managed CIP assets.

CIP BES Cyber System Review

Milestone Completed (Due: 5/4/2018 and Completed 5/3/2018)

7) [redacted] Tech Org will perform a review of all [redacted] Tech Org-managed CIP Cyber Systems and associated CIP-007 R5 documentation to ensure all accounts are identified, inventoried, and meet the CIP-007 R5.2, R5.3, and R5.4 requirements.

Closure Package

Milestone Completed (Due: 5/30/2018 and Completed 5/18/2018)

8) [redacted] Operations Compliance will complet[redacted] comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and set lement of this potential violation.

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):

(i) There are no known additional risks or impacts to the BPS while the actions in this mitigation plan are being completed.
(ii) [redacted] does not plan [redacted] plement additional actions that would increase risks to the reliability of the BPS as part of this mitigation plan.

[redacted] assesses this issue posed [redacted] nimal actual risk, and not a serious or substantial risk to the reliability of the bulk electric system. These [redacted] EA[redacted]S servers are used for log aggregation, logical access monitoring and alerting, an[redacted] inoperability or unavailability would have impacted [redacted] bility to receive and respond to alerts in accordance with CIP-007-6 R4. These EACMS servers are not ESP firewalls or EACMS Intermediate Systems used in electronic access co[redacted] to BES Cyber Assets or S[redacted] an actual impact on the reliable operation of those systems. The [redacted] servers are physically protected within a PSP, and are segmented by a separate domain, [redacted] Transmission Substations EACMS Cy[redacted] Assets associated with Medium Impact BES Cyber Systems. The layered security protections of residing in the [redacted] domain minimizes the actual possibility of unauthorized access or the introduction of malicious code on these devices.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitiga ion 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 will minimize the probability of future violations of the same requirements by reinforcing with identified personnel their res[redacted] ibilities under [redacted] policies and procedures, and by updating departmental work practices to provide additional instruction on account management for Tech Org-managed CIP assets.
[redacted] nally submitted self-report, [redacted] Technology Organization has completed the following actions to prevent future recurrence: [redacted]
2) [redacted] Tech Org, Risk and Compliance Analyst will conduct a review session with the [redacted] Tech Org personnel responsible for changing the [redacted] account password and the importance of compliance with the CIP Program. Complete 1/2/2018
5) [redacted] Tech Org will modify the [redacted] work practice to provide more specific instruction for account ide[redacted] d password change requirements. Complete 2/8/2018 [redacted]
6) [redacted] Tech Org leadership will conduct reinforcement counselling with personnel responsible for account manage[redacted] Tech Org managed CIP assets. Complete 3/12/2018

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 SERC and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
  - I am [redacted] of [redacted]
  - I am qualified to sign this Mitigation Plan on behalf of [redacted]

- I understand [redacted] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendixe 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 SERC and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

SERC Single Point of Contact (SPOC)

VIEW MITIGATION PLAN CLOSURE: CIP-007-6 (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 7/23/2018

This item was marked ready for signature by [redacted] on 7/23/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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
R5.	SERC2018-402985	SERC2018019200

Date of completion of the Mitigation Plan:

[redacted]

Training

Milestone Completed (Due: 4/5/2018 and Completed 3/12/2018)
Attachments (0)

6) [redacted] Tech Org leadership will conduct reinforcement counselling with personnel responsible for account management of [redacted] Tech Org managed CIP assets.

CIP BES Cyber System Review

Milestone Completed (Due: 5/4/2018 and Completed 5/3/2018)
Attachments (0)

7) [redacted] Tech Org will perform a review of all [redacted] Tech Org-managed CIP Cyber Systems and associated CIP-007 R5 documentation to ensure all accounts are identified, inventoried, and meet the CIP-007 R5.2, R5.3, and R5.4 requirements.

Closure Package

Milestone Completed (Due: 5/30/2018 and Completed 5/18/2018)
Attachments (0)

8) [redacted] Operations Compliance will complet[redacted]omprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and set lement of this potential violation.

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

Description of Mitigating Activities:
1) [redacted] Tech Org will change the [redacted] default password on the [redacted] [redacted] devices [redacted]. Complete 12/20/2017
2) [redacted] Tech Org, Risk and Compliance Analyst will conduct a review session with the [redacted] Tech Org personnel responsible for changing the [redacted]" account password and the importance of compliance with the CIP Program. Complete 1/2/2018
3) [redacted] Tech Org will change the [redacted] default password on the [redacted] [redacted] devices [redacted]. Complete 1/8/2018
4) [redacted] Tech Org will update the CIP-007 R5.2 documentation for the (2) [redacted] [redacted] servers and the (2) [redacted] ESM Servers. Complete 1/8/2018
5) [redacted] Tech Org will modify the [redacted] work practice to provide more specific instruction for account identification and password change requirements. Complete 2/8/2018
6 [redacted] Tech Org leadership will conduct reinforcement counselling with personnel responsible for account management of [redacted] Tech Org managed CIP assets. Due 4/5/2018 Completed 3/12/2018
7) [redacted] Tech Org will perform a review of all [redacted] Tech Org-managed CIP Cyber Systems and associated CIP-007 R5 documentation to ensure all accounts are identified, inventoried, and meet the CIP-007 R5.2, R5.3, and R5.4 requirements. Due 5/4/2018 Completed 5/3/2018
8) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Due 5/30/2018 Completed 5/18/2018

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

Milestone 1: Completed 12/20/2017
[redacted], provides evidence [redacted] Tech Org changed the '[redacted] default password on the [redacted] [redacted] devices [redacted].

Milestone 2: Complete 1/2/2018
[redacted], provides the meeting notice and meeting notes documenting the completed review session wi h the [redacted] Tech

Org personnel responsible for changing the [redacted] account password was completed.

Milestone 3: Completed 1/8/2018

[redacted], provides evidence [redacted] Tech Org changed the [redacted] default password for the [redacted] devices [redacted].

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

Milestone 4: Completed 1/8/2018

[redacted] Tech Org will updated the CIP-007 R5.2 documentation for the [redacted] Connecter servers and the [redacted] Servers. Page 2 contains the [redacted] account. Page 7 contains the [redacted] Connector [redacted] account.

Milestone 5: Completed 2/8/2018

[redacted]. Provides the modified TechOrg for [redacted] Default, Generic and Shared Accounts where TechOrg added he following additional guidance: Page 2, a new section 4.1.1 Account Identification was added which describes the process for account identification and provides a link to the [redacted] diagram used for identifying accounts. Page 7, is the [redacted] diagram. Page 8, provides an email to TechOrg personnel noting changes to the [redacted] work practice.

Milestone 6: Completed 3/12/2018

[redacted] provides the training presentation and the attendee list for the reinforcement counselling / training with personnel responsible for account management of [redacted] Tech Org managed CIP assets. Multiple training sessions were completed. The final training session was completed on 3/12/2018.

Milestone 7: Completed 5/3/2018

The following documentation provides a review of all [redacted] Tech Org-managed CIP Cyber Systems and associated CIP-007 R5 documentation to ensure all accounts are identified, inventoried, and meet the CIP-007 R5.2, 5.3 and R5.4 requirements. The purpose of the reviews was to verify the accuracy of the documentation; the reviews were completed on 5/3/2018.

The following CIP Cyber Systems were reviewed; [redacted], which are PACS assets.

During the review, [redacted] Tech Org discovered additional potential issues related to CIP007-6 R5.2 and CIP-007 R5.4. Those potential issues are identified in the documentation provided along with evidence the issues have been mitigated. A scope expansion will be filed with this original issue [redacted] once the investigation of the new potential issues is completed.

Below is a summary of the evidence of the completed review provided for milestone 7.

- [redacted] pages 2-15, provides the review demonstrating the known [redacted] default / generic accounts were properly identified, inventoried, and meet the CIP-007 R5.2 and CIP-007 R5.4 requirements for the [redacted] workstations. The review resulted in the discovery of one [redacted] account enabled on each of the [redacted] PACS workstations that should have been removed. Page 4-5 shows the removal of the errant [redacted] account on one PACS workstation; Pages 6-15 repeat the same process/evidence for the other [redacted] PACS workstations. Pages 16-20 provides the "default / generic account list" documentation for the PACS assets. This documentation was not updated based on the discovery of the [redacted] account because the account was deleted, and therefore the inventory remains accurate.
- [redacted] pages 1-10, provides the review demonstrating the default / generic accounts are identified, inventoried, and meet the CIP-007 R5.2 and CIP-007 R5.4 requirements for the [redacted] servers and panels. All currently inventoried accounts and password changes were accurate for the PACS servers and panels. Pages 11-13 provides the "default / generic account list" documentation used for CIP-007-6 R5.2 for the PACS servers / panels.
- [redacted], pages 1-59, provides the review demonstrating the default/generic accounts on EACMS CIP Cyber Systems on the Tech Org [redacted] domain were identified, inventoried, and meet the CIP-007 R5.2 and CIP-007 R5.4 for the following systems: [redacted]. The first noted discrepancy is detailed starting on Page 11, another on page 33-35, pages 47-50, and pages 52-57. Pages 58-100 provides the "default / generic account list" documentation for the above identified systems. Where modifications were made to account inventories as a result of the discrepancies noted above, highlights are provided on pages 71, 76, 77, 91, 92, and 98.
- [redacted] provides the access reviews of personnel with electronic access to [redacted] Tech Org-managed CIP Cyber Systems against associated authorization records in [redacted] to ensure all individuals with electronic access were authorized.

There were no instances of unauthorized access detected for the known and inventoried accounts. As part of the scope expansion for all discovered unknown accounts, and access reconciliation will be performed on those accounts as well.

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.

VIEW SELF-REPORT: CIP-007-6 R5. (COMPLETED)

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

This item was submitted by [redacted] on 10/30/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [redacted]

NERC Registry ID: [redacted]

JRO ID: [redacted]

CFR ID: [redacted]

Entity Contact Information: [redacted]

REPORTING INFORMATION

Applicable Standard: [redacted]

Applicable Requirement: [redacted]

Applicable Sub Requirement(s): [redacted].

Applicable Functions: [redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

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

Date Possible Violation was discovered: 6/12/2017

Beginning Date of Possible Violation: 5/25/2017

End or Expected End Date of Possible Violation: 6/13/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

[redacted] group discovered a possible CIP-007-6 R5.4 issue where a new Remote Terminal Unit (RTU) (Medium Impact BES Cyber Asset/System) commissioned on 5/25/2017 at an [redacted] Transmission substation did [redacted]lt password changed and a default service account deleted at the time of commissioning. This issue was discovered as part of a post-commission review of inventory data and commissioning checklist. Upon discovery on 6/12/2017, the administrator account name / password was changed and the service account was deleted on 6/13/2017, which was 19 days after commissioning the device.

[redacted] has [redacted] BES Cyber Assets and [redacted] medium impact substations, this is the first occurrence of commissioning a new RTU BES Cyber Asset at a medium impact substation for [redacted] since the CIP V5 effective date of 7/1/2016. As part of the extent of condition review, an electronic access review between 5/25/2017 and 6/13/2017 for the RTU was completed to determine if there had been any attempted usage of the default administrator account and the service account. The review showed that the only attempted access was by a user approved for electronic access to the device when they remotely logged onto the RTU with the default administrator account and service account passwords to verify this issue existed on 6/12/2017 following discovery in the commissioning files. This was the only electronic access to the device since commissioning on 5/25/2017. Once the issue was verified, a field technician was dispatched to the substation on 6/13/2017 to change the administrator account name and passwor[redacted]CIP [redacted] and [redacted] Operations IT Security monitors all physical and [redacted]ed there were no unauthorized events at the substation during the period of May 25, 2017 and June 13, 2017. All change[redacted]rd and delete the unnecessary service during the period of May 25, 2017 and June 13 [redacted] were authorized and performed on site by [redacted] personnel.

It was determined the root cause of this issue was a failure to follow the [redacted] CIP Policy and Procedures Manual, [redacted] and the [redacted]. Both the procedure and the work practice outline the change and validation of default passwords upon commissioning of new BES Cyber Assets. To determine the extent of condition of this issue, a comprehensive review will be performed and completed by 11/14/2017 to determine if any other new devices had been commissioned at [redacted], and to confirm that all of the [redacted] necessary commissioning steps for new devices were completed.

To mitigate th[redacted]nt recurrence, [redacted] will add an attachment task list for commissioning devices to the Substatior [redacted] applicabl [redacted] on organizations. The purpose of the commissioning task list is to provide additional guidance to field personnel as devices are commissioned. Also, training on the commissioning task list attachment in the [redacted] addressing CIP-007-6 R5.4 is also scheduled for completion.

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

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

1) [redacted] Technician will change the default administration account password /name on the RTU and remove the service account [redacted] Completed 6/13/2017
2) [redacted] will perform an access review of the RTU during the period 5/25/2017 – 6/13/2017 following commissioning and when the administrator account password / name and service account was changed/removed. Completed 8/15/2017
3) [redacted] will add a commissioning task list as an attachment to the [redacted]' as an additional guide for commissioning devices. Complete by 11/14/2017
4) [redacted] will complete a review of BCA/PCA devices commissioned at medium impact substations since 7/1/2016 to verify the password requirements were met. Completed by 11/14/2017
5) [redacted] will conduct a review / training session with [redacted] and affiliate operating company personnel on the addition of the commissioning task list to the [redacted] to address CIP-007-6 R5.4. Complete by 12/5/2017
6) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Complete by 12/20/2017

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

12/20/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
WP Task List	11/14/2017	3) [redacted] will add a commissioning task list as an attachment to the [redacted]' as an additional guide for commissioning devices.	Yes
Verify PWD Rqts	11/14/2017	4) [redacted] will complete a review of BCA/PCA devices commissioned at medium impact substations since 7/1/2016 to verify the password requirements were met.	No
Retraining	12/5/2017	5) [redacted] will conduct a review / training session with [redacted] and affiliate operating company personnel on the addition of the commissioning task list to the [redacted] to address CIP-007-6 R5.4.	Yes
Closure Package	12/20/2017	6) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.	No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue posed a minimal potential risk, and not a serious or substantial risk to the reliability of the bulk electric system. Potential risk could include the introduction of unknown vulnerabilities and configuration changes susceptible to exploitation by not following documented processes and verifying security controls are in place prior to commissioning a device. The root cause of this issue was a failure to thoroughly follow new BES Cyber Asset commissioning steps to change default account passwords and remove/disable an account not needed. This oversight could have potentially allowed electronic access to the device by someone knowledgeable of the vendor default account passwords for this specific device, but those personnel would have to be physically standing at the device, which is protected within a PSP.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk, and not a serious or substantial risk to the reliability of the bulk electric system. [redacted] failure to change the administrator account password and delete the service account on the RTU could have allowed a user with authorization for physical access to the Substation PSP or electronic access the ability to modify the configuration of the RTU. However, the CIP [redacted] and [redacted] Operations IT Security monitors all physical and electronic/network events at the substation 24/7, and both confirmed there were no unauthorized events at the substation during the period of May 25, 2017 and June 13, 2017. There were no unauthorized events at [redacted] during the period of May 25, 2017 and June 13, 2017. Any change to a RTU configuration generates a file comparison with the previous file. After the comparison, an email is sent to [redacted] to notify them of the file change and includes details of what changed. There were no unauthorized changes to the RTU configuration during the period in question. In addition to monitoring, the device is physically protected within a PSP, and other logical protections for other devices within the PSP are in place to further minimized the actual possibility introduction of unknown vulnerabilities and configuration changes.

Additional Comments:

[redacted], [redacted] that address CIP-007-6 R5.4: [redacted]

• Section 4.1 (Planning for a NEW Cyber System), Section 4.1.8, (Baseline Configuration), Step 10
10. Identify all default or other generic accounts available on the CIP Cyber System which includes vendor supplied default accounts and accounts set up by an operating system or application to perform specific operations that individual users do not receive authorization to use. Each account must be removed or disabled or renamed [redacted]re pos[redacted]le. For those accounts th[redacted] cannot be removed, or disabled, the password must be changed. If a password cannot be changed without affecting functionality, document this [redacted] vendor manuals or vendor statements. All default or other generic accounts that remain enabled must be documented per section 5.7, Evidence for Each Default or Generic Account.
• Section 4.2, Commission CIP Cyber Systems, Step 14
14. Change all known default passwords and validate that the passwords have been changed.

Substation System [redacted]

1. The applicable [redacted] group shall implement CIP compliant passwords on all applicable BES Cyber Assets, [redacted] Connectors and/or Protected Cyber Assets [redacted] dual can gain electronic access to any of these devices until the individual's logon credentials have been properly authenticated for interactive access.
• Section 3.2, Identify and Inventory All Known Enabled Default or Othe[redacted]s [redacted] [redacted] [redacted]licable [redacted] shall either rename, remove or disable all enabled default and/or generic accounts or at least change their default passwords provided by the vendor for each applicable Cyber Asset.
• Section 3.4.2, Commissioning a New BES Cyber Asset that is part of a mediu[redacted] [redacted]otected Cyber Asset and/or [redacted]

Connector
The following shall be performed when commissioning a new BES Cyber Asset that is part of a medium impact BES Cyber System and its associated Protected Cyber Asset and/or [redacted]:
[redacted]pplicable [redacted] group shall change all the default passwords [redacted] generated.
[redacted]

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

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW MITIGATION PLAN CLOSURE: CIP-007-6 (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 12/6/2017

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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
R5.	SERC2017-402876	SERC2017018548

Date of completion of the Mitigation Plan:

[redacted]

[redacted] Task List

Milestone Completed (Due: 11/14/2017 and Completed 11/13/2017)
Attachments (0)

3) [redacted] will add a commissioning task list as an att[redacted]e[redacted]o the [redacted]' as an additional guide for [redacted]

Verify [redacted]

Milestone Completed (Due: 11/14/2017 and Completed 11/8/2017)
Attachments (0)

4) [redacted] will complete a review of BCA/PCA devices commissioned at medium impact substations since 7/1/2016 to verify the password requirements were met.

Retraining

Milestone Completed (Due: 12/5/2017 and Completed 11/30/2017)
Attachments (0)

5) [redacted] will conduct a review / training session with [redacted] and [redacted]missioning task list to the [redacted] to address CIP-007-6 R5.4.

Closure Package

Milestone Pending (Due: 12/20/2017)
Attachments (0)

6) [redacted] [redacted]erations Compliance will complete a compre[redacted]s[redacted]review [redacted]d prepare a summary closure [redacted]n.

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

Description of Mitigating Activities: 1) [redacted] Technician will change the default administration account password /name on the RTU and remove the service account [redacted]. Completed 6/13/2017
2) [redacted] will perform an access review of the RTU during the period 5/25/2017 – 6/13/2017 following commissioning and when the administrator account password / name and service account was changed/removed. Completed 8/15/2017
3) [redacted] will add a commissioning task list as an attachment to the [redacted]' as an additional guide for commissioning devices. Complete by 11/14/2017
4) [redacted] will complete a review of BCA/PCA devices commissioned at medium impact substations since 7/1/2016 to verify the password requirements were met. Completed by 11/14/2017
5) [redacted] will conduct a review / training session with [redacted] and affiliate operating company personnel on the addition of the commissioning task list to the [redacted] to address CIP-007-6 R5.4. Complete by 12/5/2017
6 [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Complete by 12/20/2017

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

Milestone 1: Completed 6/13/2017
[redacted], page 1 provides evidence the [redacted] Technician changed the default administration account name from "Administrator" to "[redacted] in addition the password was changed. Page 2 provides evidence the account [redacted] was deleted.

Milestone 2: Completed 8/15/2017

[redacted], provides an access review of the RTU during the period 5/25/2017 – 6/13/2017. There were two login [redacted] event logs and one logoff event on the RTU during this timeframe. These events were done by the [redacted] analyst investigating this issue and were related to him changing the default administrator account name and password, and deleting the "[redacted]" account. No other login activity was observed after the device was commissioned.

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

Milestone 3: Completed 11/13/2017

[redacted] provides the modified work practice where [redacted] added a commissioning task list as an attachment to the [redacted]'.

Milestone 4: Completed 11/8/2017

[redacted] pages 1-3 provides the review [redacted] completed for BCA/PCA devices commissioned at medium impact substations since 7/1/2016 to verify the password requirements were met. The spreadsheet contains a list of all devices commissioned after 7/1/2016 (Column: Commission Date) and verification the default password was changed (Column: Default Password Changed). Page 4 provides evidence of a password change for one of the devices selected in the list, which is highlighted for reference ([redacted]).

Milestone 5: Completed 11/30/2017

[redacted], page 1 provides the meeting notice for the review / retraining for the addition of the commissioning task list to the [redacted] to address CIP-007-6 R5.4. Page 2, provides the agenda for the training. Page 3 provides the attendee list for training and the date completed.

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.

VIEW SELF-REPORT: CIP-007-6 R5. (COMPLETED)

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

This item was submitted by [redacted] on 10/6/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:	[redacted]
NERC Registry ID:	[redacted]
JRO ID:	[redacted]
CFR ID:	[redacted]
Entity Contact Information:	[redacted]

REPORTING INFORMATION

Applicable Standard:	[redacted]
Applicable Requirement:	[redacted]
Applicable Sub Requirement(s):	[redacted]
Applicable Functions:	[redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered:	No
Has this Possible Violation previously been reported to other Regions:	No
Date Possible Violation was discovered:	7/26/2016
Beginning Date of Possible Violation:	7/1/2016
End or Expected End Date of Possible Violation:	8/25/2016
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

On July 26, 2016 the [redacted] IT [redacted] group was comple ing a Cyber Security Controls Pre-verification review related to a configuration change case. During the review it was determined the minimum password length setting for domain users was set to a value of seven (7). The domain policy configuration for [redacted] was then changed on July 27, 2016 to a minimum password length setting of eight (8).

Between July 1, 2016 and July 27, 2016, the password length and complexity requirements for password-only authentication were procedurally enforced on the [redacted] for members of the [redacted] Information Technology group using the work practice [redacted] pages 9 -10. The [redacted] is a segmented domain managed by [redacted] IT and hosting Transmission EACMS Cyber Assets associated with Medium Impact BES Cyber Systems. The total number of in-scope Cyber Assets on the [redacted] using password-only authentication was [redacted] out o [redacted] total.

Between August 24th, 2016 and September 22nd, 2016, a review of user accounts associated with the domain policy was completed, and one user was found to have a domain password set to less than the 8 character minimum. For the one user, their password was changed on August 25th, 2016 to meet compliance with the 8 character minimum.

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

1) To prevent future recurrence of issues associated with procedural enforcement of the 8 character password minimum, [redacted] IT modified the [redacted] to technically enforce a password length of 8 characters for all [redacted] users where password-only authentication is used. Completed 7/29/2016

2) To determine the extent of condition, [redacted] IT completed a review of all [redacted] user's account passwords used on the [redacted] to determine if any users were using a password less than 8 characters in length. Completed 9/22/2016

3) [redacted] IT required the one user found using a password less than 8 characters in length to change their password based on the updated [redacted] Completed 8/25/2016

Provide details to prevent recurrence:

Execution of the above stated mitigation plan milestones will prevent future recurrence of this issue.

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

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

9/22/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue posed a minimal potential risk, and not a serious or substantial potential risk to the bulk power system. Potential risk could include possible compromise of a weak password; however the Cyber Assets on the [redacted] using password-only authentication do not provide any control functionality or Interactive Remote Access capability. The Cyber Assets in question using password-only authentication included log aggregators used in CIP-007-6 R4 – [redacted] and [redacted] hosts where unauthorized electronic access due to compromise of a weak password could have included the ability to view or change the operating system characteristics of the running services for the [redacted] but not the event monitoring itself. Likewise, the [redacted] hosts and [redacted] access provided the ability to change the characteristics of the [redacted] host operating systems and the [redacted] allocations and properties of any hosted [redacted] but no in-guest access to the [redacted] was afforded.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk and did not pose a serious or substantial actual risk to the reliability of the bulk power system. This issue was a result of one employee not following procedures implemented as of July 1, 2016 with regard to password length. As a result, [redacted] IT implemented technical controls within 27 days to change the [redacted] group policy object to enforce an eight character password minimum on in-scope devices. The employee found to have a seven character password is still within [redacted] IT, has met all of the required pre-requisites for access, and maintains the same electronic access they had prior to the domain policy change. This potential issue is considered to be a result of a human performance deficiency addressed through technical enforcement of the required password minimum.

Additional Comments:

[redacted]

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW MITIGATION PLAN CLOSURE: CIP-007-6 (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 10/26/2016

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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
R5.	SERC2016-402499	SERC2016016339

Date of completion of the Mitigation Plan:

[redacted]

No Milestones Defined

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

Description of Mitigating Activities:
1) To prevent future recurrence of issues associated with procedural enforcement of the 8 character password minimum, [redacted] IT modified the [redacted] to technically enforce a password length of 8 characters for all [redacted] domain users where password-only authentication is used. Completed 7/29/2016
2) To determine the extent of condition [redacted] IT completed a review of all [redacted] user's account passwords used on the [redacted] domain to determine if any users were using a password less than 8 characters in length. Completed 9/22/2016
3) [redacted] IT required the one user found using a password less than 8 characters in length to change their password based on the updated [redacted] Completed 8/25/2016

Details to Prevent Recurrence: Execution of the above stated mitigation plan milestones will prevent future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

Milestone 1
[redacted] page 2, document includes screenshot evidence that the [redacted] was changed from 7 characters to 8 characters on 7/27/2016.

[redacted] document includes evidence of the change case completed on 7/29/2016 to modify the [redacted] policy set from 7 characters to 8 characters

Milestone 2
[redacted] document includes evidence of a review of those users associated with the [redacted]. This review was completed on 9/22/2016. 1 user [redacted] was found to have a password with less than 8 characters.

Milestone 3
[redacted] document includes evidence the user [redacted] completed a password change on 8/25/2016 to modify the existing password length to 8 characters.

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.

Attachment 13

Record documents for the violation of CIP-010-2 R1

13a. The Entities' Self-Report (SERC2016016321)

13b. The Entities' Mitigation Plan designated as SERCMIT014426 submitted February 8, 2019

13c. The Entities' Certification of Mitigation Plan Completion submitted February 8, 2019

13d. The Entities' Self-Report (SERC2018019106)

13e. The Entities' Certification of Mitigation Plan Completion submitted April 27, 2018

VIEW SELF-REPORT: CIP-010-2 R1. (COMPLETED)

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

This item was submitted by [redacted] on 9/30/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [redacted]

NERC Registry ID: [redacted]

JRO ID: [redacted]

CFR ID: [redacted]

Entity Contact Information: [redacted]

REPORTING INFORMATION

Applicable Standard: [redacted]

Applicable Requirement: [redacted]

Applicable Sub Requirement(s): [redacted]

Applicable Functions: [redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered: [redacted]

Has this Possible Violation previously been reported to other Regions: [redacted]

Date Possible Violation was discovered: [redacted]

Beginning Date of Possible Violation: [redacted]

End or Expected End Date of Possible Violation: [redacted]

Is the violation still occurring? [redacted]

Provide detailed description and cause of Possible Violation:

While responding to a Level 2 Data Request in preparation for [redacted] upcoming SERC CIP audit, it was discovered that [redacted] Transmission [redacted] inadvertently failed to list an authorized enabled port in baseline documentation. [redacted] Transmission was aware that this port was open, and has a valid business justification for the use of this port, as shown in [redacted] Transmission's firewall rules documentation. The port in question is used to send device logs from non-[redacted] systems to an [redacted] log aggregator, and was documented in previous versions of [redacted] Transmission baseline documentation. Due to an inadvertent transcription error when transferring data to a new spreadsheet, this port was errantly left off and was not listed on the July 1, 2016 version of the [redacted] Transmission baseline documentation. The [redacted] Transmission baseline documentation was updated on September 6, 2016 to include the port in question. The scope of noncompliance is limited to a documentation error from July 1 through September 6, 2016 (68 Days).

Are Mitigating Activities in progress or completed? [redacted]

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

1. Update [redacted] Transmission baseline documentation to include the open port. (Completed 9/6/16)
2. Review [redacted] Transmission baseline documentation to ensure all authorized logical network accessible ports are included. (10/14/16)
3. Implement a secondary Supervisor review of any changes to the Transmission baseline documentation and business justifications to ensure all ports enabled and required for operations are included in the associated baseline documentation. Supervisory review shall be captured in the baseline change log. (10/31/16)

Provide details to prevent recurrence:

Execution [redacted] ion steps will correct the issue and prevent future recurrence.
[redacted]

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

10/31/2016

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

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Update Baseline Docs	9/6/2016	Update [redacted] Transmission baseline documentation to include the open port.	No
Review All Other Baseline Docs	10/14/2016	Review [redacted] Transmission baseline documentation to ensure all authorized logical network accessible ports are included.	No
Supervisor Review Process	10/31/2016	Implement a secondary Supervisor review of any changes to the Transmission baseline documentation and business justifications to ensure all ports enabled and required for operations are included in the associated baseline documentation. Supervisory review shall be captured in the baseline change log.	Yes

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue poses a minimal potential risk, and not a serious or substantial potential risk to the bulk power system. [redacted] to send device logs from non-[redacted] systems to an [redacted] log aggregator. The noncompliance issue is limited to a documentation er[redacted]rt information was errantly omitted in the Transmission Substation's baseline documentation used for CIP-010-2 R1.1, the port and its business justification were included in the CIP-005-5 R1.3 firewall rulesets.

Provide detailed description of Actual Risk to Bulk Power System:

This issue poses a minimal potential risk, and not a serious or substantial potential risk to the bulk power system. [redacted] Transmission was aware of the port [redacted]on and had a va[redacted]ness justification for this port to be open/enabled. A thorough review of the [redacted] Transmission baseline determined that all other logical network accessible ports were properly documented.

Additional Comments:

[redacted] [redacted] [redacted] [redacted]

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW FORMAL MITIGATION PLAN: CIP-010-2 (REGION REVIEWING MITIGATION PLAN)

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

This item was signed by [redacted] on 2/8/2019

This item was marked ready for signature by [redacted] on 2/8/2019

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-010-2 R1.	SERC2016016321	SERC2016-402496	09/30/2016	Revision Requested	Informal	
CIP-010-2 R1.	SERC2016016321, SERC2016016451	SERC2016-402496, SERC2016-402520	01/15/2019	Revision Requested	Formal	1
CIP-010-2 R1.	SERC2016016321, SERC2016016451	SERC2016-402496, SERC2016-402520	02/08/2019	Region reviewing Mitigation Plan	Formal	2

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

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

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

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name: [redacted]

Company Address: [redacted]

[redacted]

Compliance Registry ID: [redacted]

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

Name: [redacted]

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

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

Standard: [redacted]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R1.	SERC2016-402496	SERC2016016321	[redacted]
R1.	SERC2016-402520	SERC2016016451	[redacted]

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

While responding [redacted] 2 Data Request in preparation for [redacted] upcoming 2016 SERC CIP audit, the [redacted] s part of [redacted], discovered on [redacted] advertent failure to list a [redacted] uthorized enabled port [redacted] in baseline d [redacted] baseline grouping of [redacted] mpact EACMS devices used across [redacted] in the [redacted] medium impact Substations. The [redacted] in question is used to se [redacted] gs from [redacted] systems to an [redacted] log aggregator and was documented in previous versions of [redacted] baseline docume [redacted] transcription error when transferring data to a new spreadsheet, this port was [redacted] off of the new list and was not [redacted] y 1, 2016 version of the [redacted] baseline documentation. [redacted] was aware that this port was open and has a valid business justification for the use of this port prior to the 7/1/2016 CIP V5 effective date, as shown in [redacted] firewall rules documenta [redacted] n. The [redacted] baseline documen [redacted] or [redacted] nber 6, 2016 to include the port in question. The original scope of nonc [redacted] n error from July 1 through Septemb [redacted] s). [redacted]

Prior to the 2016 SERC CIP Audit onsite review, the [redacted] g [redacted] t of Milestone 2 of he associated mitigation plan for SERC issue [redacted], discovered an [redacted] tional enabled por [redacted] that wa [redacted] also missing in the baseline gr [redacted] r the [redacted] devices. This discovery and associated documentation up [redacted] was provided as pa [redacted] e evidence in the closure package for the ass [redacted] ed mitigation plan, and this was also dis [redacted] ith the auditors duri [redacted] CIP audit. [redacted]

During the 2016 SERC CIP Audit o [redacted] while auditing the closely related CIP-007 R1, auditors found two p [redacted] e violations of the same requirement pa [redacted] was also found to be open, but not li [redacted] e baseline configurat [redacted] n the sampled Cyber Asset [redacted] This is the same device ty [redacted] C issue [redacted] ut deals wi [redacted] ent port [redacted] wh [redacted] needed t [redacted] led on [redacted] gement an [redacted] vice whitelisting b [redacted] product.

2) An overly broad port range was specified in the baseline configuration for the sampled Cyber Asset [redacted]. Upon fur[redacted] ined this rang[redacted] have been only [redacted]. This Cyber Asset is maintained by the EMS business unit, whereas the Cyber Asset involved in the OEA/self-report is maintained by the [redacted] business unit. As noted by the SERC Audit Team, "The issue involving an overly broad port range was als[redacted] imple documentation error; no[redacted] f the unnecessary [redacted]

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

In [redacted]rst issue, the bas[redacted] cross [redacted] medium im[redacted] Substations out of a total of approximately [redacted] CIP substation devices at the time. The baseli[redacted] docu[redacted]tion at the time was managed by the [redacted] group, while the second sampled asset, [redacted] represents [redacted] act Control Centers/datacenters out of ap[redacted]mately [redacted] CIP control center devices at that time that resides with [redacted] is managed by the [redacted] Energy Management System business unit.

Additionally, the following provides information related to the previously submitted [redacted] issues.

On 8/22/2016, [redacted] Technology Organization [redacted] discovered a potential violation of CIP-010-2 R1.1 when performing a security controls verification prior to installing a [redacted] security patch. Prior to the installation of the patch, a port scan revealed [redacted] to be open, although this port was not in the baseline documentation as an authorized port in accordance with CIP-010-2 R1.1. The [redacted] Hosts CIP cyber system is an EACMS associated with Transmission Substation medium impact BES Cyber Systems and consists of [redacted] host servers. The initial ports and services whitelist evidence document for these servers was created on 2/26/2016, prior to and in preparations for the CIP V5 effective date. At that time, the [redacted] version was 5.5; however, a system upgrade was performed on 4/20/2016 to upgrade the version to [redacted] required [redacted] to be open in addition to the documented [redacted] for High Availability/Fault Tolerance features of [redacted]. Following the upgrade on 4/20/2016, the ports and services whitelist document, which is a component of the R1.1 baseline configuration documentation, should have been updated prior to July 1, 2016 when these servers were commissioned under CIP V5. Upon detection of the discrepancy on 8/22/2016, the ports and services whitelist was updated on 8/25/2016 to add [redacted] as a required and authorized enabled port.

This potential issue is considered a documentation error due to [redacted] Tech Org personnel failure to follow [redacted] NERC CIP procedure [redacted] provide instruction on determining and documenting the information required for baseline configuration. In this particular case, a review of documentation should have been performed after the upgrade on 4/20/2016 and prior to the commission date of 7/1/2016 to confirm baseline documentation was accurate on the date of commissioning.
As part of Scope Expansion #1 filed on 5/18/2017 for issue SERC [redacted] self-reported on 11/3/2016, the following additional issues were discovered:

(1) PACS associated with [redacted] and [redacted] Security Patches
On 8/8/2016, [redacted] Technology Organization [redacted] discovered [redacted] Operating System security patches determined to be applicable on 7/12/2016 for one PACS server that were scheduled for deployment on or before 8/16/2016; however, the patches were deployed ahead of schedule and outside of the organization's CIP Change Management process on 08/04/2016. The patches were inadvertently added to a [redacted] Security Patch Deployment "roll-up" group and as a result, authorization for the deployment and installation of the patches was not completed at the time of the change. Additionally, an evaluation of impacted cyber security controls was not completed prior to the patches being installed in accordance with CIP-010-2 R1.4. The cyber security controls verification for the PACS server was completed as of 8/29/2016, which was 25 days after installation of the patches.
Updates to the baseline configuration documentation for the PACS server were due on 09/03/2016 in accordance with CIP-010-2 R1.3, but were not completed until 9/8/2016. This potential issue is considered a failure to ensure that these PACS assets were not susceptible to unauthorized changes initiated on the corporate network, and a failure by [redacted] Tech Org personnel to follow [redacted] procedure. Mitigation of this issue involved excluding these PACS assets from the enterprise deployment [redacted] collections and adding them to a PACS systems collection for all future targeted security patch deployments.

(2) EACMS associated with Substation [redacted]
On 8/26/2016, [redacted] Technology Organization [redacted] discovered a potential violation of CIP-010-2 R1.2 while performing a cyber security controls verification in preparation for a security patch deployment. [redacted] IT discovered that the [redacted] agent software and the accompanying [redacted] software were upgraded on [redacted] EACMS servers associated with Transmission Substation Medium Impact BES Cyber Systems outside the organization's CIP Change Management (CM) process on 8/15/2016. These [redacted] EACMS servers support the [redacted] application (Intermediate System) used for Interactive Remote Access (IRA) to 'medium' Substations. The software upgrade occurred because the [redacted] EACMS servers were part of an enterprise managed group of all [redacted] Tech Org-managed [redacted] servers. Therefore, authorization for the software upgrade on the [redacted] EACMS servers was not completed at the time of the change. Since the upgrade occurred outside of the CM process, no pre- or post-change cyber security controls verification was performed at the time of the change as per CIP-010-2 R1.4. The cyber security controls verification for these [redacted] EACMS servers was completed on 9/14/2016, which was 29 days after he upgrade of the software. The baseline documentation for these [redacted] EACMS servers was updated on 9/2/2016 within 30 days of the change in accordance with CIP-010-2 R1.3. This potential issue is considered a failure to follow [redacted]. In this particular case, a review should have been performed prior to and following the change to ensure the upgrades did not adversely impact applicable cyber security controls, and to obtain the required authorization for the upgrades. Mitigation of this issue included removing all EACMS [redacted] servers from the existing enterprise management containers and changing them to the new CIP EACMS containers for future backup agent deployments.

(3) PACS associated with [redacted] Upgrade
On 10/6/2016, [redacted] Technology Organization [redacted] discovered while performing a cyber security controls verification prior to a device change that a [redacted] software upgrade had been deployed to [redacted] PACS servers ([redacted] on 8/18/2016 | [redacted] on 9/13/2016) and [redacted] PACS monitoring workstations ([redacted] on 08/19/2016 | [redacted] on 09/23/2016 | [redacted] on 08/19/2016 | [redacted] on 08/19/2016 [redacted] on 08/23/2016 [redacted] on 08/18/2016). The variation in installation dates corresponds with device reboots. The [redacted] software upgrade from [redacted] on these [redacted] PACS assets was a result of an enterprise deployment pushed out on the corporate [redacted] domain. This deployment was unintended and occurred because the Active Directory Software Deployment [redacted] for PACS servers and workstations leveraged the same [redacted] package used for the enterprise [redacted] software deployment. As a result, authorization for the upgrade of this software on these eight assets was not completed at the time of the change. Additionally, pre- and post-change cyber security controls verifications were not completed at the time of the change as per CIP-010-2 R1.4. Baseline documentation updates as per CIP-010-2 R1.3 to reflect the new version of software were completed as follows:

- [redacted] on 10/7/2016, which was 50 days after the initial upgrade on 8/18/2016
- [redacted] on 10/7/2016, which was within 30 days of the change on 9/13/2016
- [redacted] on 10/7/2016, which was 49 after the change on 8/19/2016
- [redacted] on 10/7/2016, which was within 30 days of the change on 9/23/2016
- [redacted] on 10/7/2016, which was 49 days after the change on 8/19/2016
- [redacted] on 10/7/2016, which was 49 days after the change on 8/19/2016
- [redacted] on 10/7/2016, which was 53 days after the change on 8/23/2016
- [redacted] on 10/7/2016, which was 48 days after the change on 8/18/2016

The cyber security controls verification for the [redacted] PACS servers was completed on 8/30/2016 (12 days after the change), and 9/13/2016 (same day), respectively. The root cause of this issue was the unknown susceptibility of these PACS assets to enterprise-wide [redacted] deployments and is considered a failure to follow [redacted] procedure. Mitigation of this issue will include exempting all PACS servers and workstations from the enterprise-wide [redacted] group policy installations.

(4) EACMS associated with Substation [redacted]
On 1/5/2017, [redacted] Technology Organization [redacted] discovered a potential violation of CIP-010-2 R1.1 where software installed on [redacted] servers was not properly captured in the baseline documentation for those servers. The issue was discovered while preparing for upgrades to installed software on these servers. The installed software not reflected in baseline documentation included [redacted] which is Authentication Services provided by [redacted] and [redacted] which is the [redacted]. Both servers (out of [redacted] CIP severs managed by [redacted] IT) are EACMS associated with Transmission Substation Medium Impact BES Cyber Systems, and are used in the CIP-007-6 R4 Security Event Monitoring processes. Upon discovery [redacted] IT determined that the software in question was installed prior to 7/1/2016, but was not included in any previous versions of baseline documentation for these assets following commissioning of these devices under CIP V5 on 7/1/2016. Additionally, the software and it's absence from all previous versions of baseline documentation for these devices was not detected and updated at the time of the attested completion of [redacted] Tech Org-managed device baseline documentation reviews in accordance with the milestone due 11/18/2016 as part of open issue SERC [redacted]. To mitigate this issue, baseline documentation updates to reflect this software was completed on 1/5/2017. As a result of this new discovery, [redacted] is proposing the below updated mitigation plan milestones to address this expansion of scope of the original issue.

(5) PACS associated with [redacted]
On 2/27/2017, [redacted] Technology Organization [redacted] discovered a potential violation of CIP-010-2 R1.1 where, in preparation for the annual BES Cyber System and associated Cyber Asset review and update, it was found that [redacted] PACS controller panels at a CIP PSP [redacted] were commissioned on 4/20/2016 but not added to the PACS asset list until 3/9/2017. This resulted in the baseline documentation for each of the [redacted] added panels not being captured and correct on the effective date of CIP-010-2 R1 on July 1, 2016, but [redacted] days later. In addition, [redacted] PACS controller panels at [redacted] different CIP PSPs had their firmware upgraded on 4/21/2016 ([redacted] 5/9/2016 [redacted]), and 11/22/2016 ([redacted]), respectively. The newer firmware version on each of these [redacted] PACS controller panels was not reflected in the applicable baseline documentation for the PACS assets until 3/9/2017, which in the longest case was [redacted] days after the required timeframe to update the baseline documentation. For the PACS controller panel firmware upgrade that occurred on 11/22/2016, there was no record of authorization at the time the upgrade was performed as per R1.2. As part of milestone 9 of scope expansion #1, [redacted] Tech Org completed a review and security control verification for these [redacted] panels as of 3/23/2017; there was no pre-change security controls review performed at the time of the change on 11/22/2016. As part of milestone 14 of scope expansion #1, and to determine the extent-of-condition of this issue, [redacted] Tech Org completed a review of all PACS assets to verify all controls and baseline documentation was accurate, completed as of 6/29/2017.

To prevent future recurrence of this issue, [redacted] Tech and the Physical Security Operations Team (PSOT) conducted retraining sessions with OPCO Corporate Security groups on the PACS configuration change management process. The root cause of this issue was a failure on the part of the PSOT and personnel within the OPCO Corporate Security groups to properly coordinate and document changes to PACS controller panels at the time of the change in accordance with [redacted], and CIP-010-2 R1.

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

As part of Scope Expansion #2 filed on 9/15/2017 for issue SERC [redacted] filed on 11/3/2016, the following additional issues were discovered:
On 6/14/2017, the [redacted] Technology Organization (Tech Org) discovered potential issues related to CIP-010-2 R1. These issues were all discovered as part of a baseline documentation review for [redacted] PACS PSP monitoring workstations and [redacted] servers in accordance with existing self-report/mitigation plan milestone #14 in open issue SERC [redacted] Scope Expansion of [redacted]) due 6/29/2017. The purpose of the milestone was to verify the accuracy of baseline documentation for all [redacted] Tech Org-managed CIP cyber systems. The following provides a summary of the issues discovered during the analysis for milestone 14 for these [redacted] PACS assets and [redacted] [redacted] servers.

(6) Ports and Services
On 6/9/2017, the [redacted] Tech Org discovered a potential issue of CIP-010-2 R1.1 when a port scan of [redacted] PACS assets revealed [redacted] to be open, although these ports were not in the baseline documentation ports and services whitelist as authorized. It was determined these ports were enabled as of the CIP V5 effective date of 7/1/2016, however the port scanning method previously used failed to recognize these ports as enabled because the original script prevented the identification of the higher range [redacted], and the [redacted] scan being performed remotely was masking the identified ports. The ports were discovered on 6/9/2017 using an updated version of the script and the [redacted]t utility.
Upon detection of the discrepancy on 6/9/2017, the baseline documentation ports and services whitelist for these [redacted] PACS assets was updated on 6/21/2017 to add [redacted] and high [redacted] after these were determined to be required and authorized ports. [redacted] and the [redacted] are associated with the [redacted] service, a required [redacted] component, and [redacted] is associated with the [redacted] service, a required [redacted] component. Therefore, this issue is viewed as a documentation issue as per CIP-010-2 R1 as all ports and services discovered open were needed to be enabled.
In order to mitigate this issue, the [redacted] Tech Org deployed new technical controls on 6/9/2017 to perform a comparison between the baseline configuration ports and services whitelist and the listening ports and services derived from the output of the [redacted] command. This new control will flag any listening port or installed [redacted] service that is not consistent between the approved ports and services whitelist and the listening ports and services. This new control also provides additional mitigating oversight improvements to visual comparisons between the ports and services whitelist and the previous output of listening ports and services.

(7) [redacted] Agent
On 6/9/2017, the [redacted] Tech Org discovered a potential issue of CIP-010-2 R1.1 where software installed on [redacted] PACS workstations was not properly captured in the baseline documentation software inventory. The installed software not reflected in baseline documentation was an [redacted] agent installed on each asset used for [redacted] authentication. The [redacted] Tech Org determined that the [redacted] software was installed prior to 7/1/2016; however, the software was not included in any previous versions of installed software inventories in the baseline documentation for the [redacted] assets following commissioning of these devices under CIP V5 on 7/1/2016. The confirmation of security controls occurred as part of Milestone 14 of scope expansion #1 for [redacted], which stated [redacted] IT will perform a review of all [redacted] and PACS baseline documentation, and verify all are up to date and accurate." CIP-010-2 R1 [redacted] demonstrates [redacted] IT completed a review of all PACS assets to verify all controls and baseline documentation was accurate, completed as of 6/29/2017.
To mitigate this issue, the baseline documentation software inventory was updated to reflect this installed software on 6/21/2017. To correct and prevent the future omission of installed software on in-scope assets, the [redacted] Tech Org implemented technical controls on 6/9/2017 to perform a line by line comparison between the baseline documentation software inventory and the software installed on the workstations.
This new control will flag any software component or software version that is not consistent between the software inventory baseline documentation and the installed software. This new control mitigates human performance errors by providing a more automated technical solution to eliminate oversight in a visual comparison between the software inventory and the installed software.

(8) [redacted]
On 6/9/2017, the [redacted] Tech Org discovered a potential issue of CIP-010-2 R1.1 where a software upgrade was installed on [redacted] PACS workstations on 4/22/2017, but the baseline documentation for these assets was not updated to reflect the software upgrade until 6/22/2017, 31 days after the required timeframe to update the baseline documentation. The baseline documentation reflected [redacted] but the upgrade applied [redacted]. The software upgrade was authorized as per CIP-010-2 R1.2 on 4/11/2017; pre- and post-change security controls checks were performed on 3/23/2017 and 5/1/2017, with no identified issues. This issue is considered a documentation error because an analyst performing the updates failed to save the updated baseline documentation spreadsheet in the document repository.

(9) [redacted]
On 6/14/2017, the [redacted] Tech Org discovered a potential issue of CIP-010-2 R1.2 where [redacted] software was installed on [redacted] PACS workstations on 5/18/2017 outside the organization's CIP change management process. The software installation occurred because an analyst failed to include the [redacted] PACS workstations located at [redacted] [redacted] security base in an exclusion list in one of the deployment jobs created to install the application across the enterprise. The [redacted] software was not needed and should not have been installed on these PACS assets because these [redacted] assets use [redacted] for malicious code prevention. Upon discovery, the [redacted] Antivirus software was uninstalled on 6/15/2017 following proper change management processes.

On 6/20/2017, the [redacted] Tech Org discovered another potential issue of CIP-010-2 R1.2 where [redacted] software was installed on [redacted] PACS workstations outside the organization's CIP change management process on 2/22/2017 and 2/24/2017, respectively. The software installation occurred because the [redacted] workstations were part of an enterprise managed group that should have been, but were not excluded from these deployments. Upon discovery, the [redacted] software was determined to not be needed on these workstations and was uninstalled on 6/22/2017 following proper change management processes.

In both cases, authorization for the software installation was not completed at the time of the change in accordance with CIP-010-2 R1.2, and no pre- or post-change cyber security controls verification was performed at the time of the change as per CIP-010-2 R1.4 because these changes were unintended and unexpected for these PACS assets. In order to mitigate these issues, on 7/20/2017, configuration changes to the [redacted] were made which restricted who can deploy software and patches to PACS assets going forward. Also, the Technology Services organization has created new workstation collection groups that will better enforce the exclusion of PACS assets from enterprise deployments going forward.

(10) [redacted]
On 6/14/2017, the [redacted] Tech Org discovered a potential issue of CIP-010-2 R1.3 where [redacted] software uninstalled on [redacted] [redacted] [redacted] servers on 4/18/2017 was not properly removed from the baseline documentation for those servers within 30 days of the uninstallation. The update to the baseline documentation was completed 6/14/2017, which was 27 days after the required timeframe of 30 days (57 days total). The [redacted] [redacted] servers are EACMS associated with Transmission Substation Medium Impact BES Cyber Systems. The servers are used in the CIP-007-6 R4 Security Event Monitoring processes for logging and alerting of the required security events. The [redacted] software was uninstalled because it was being replaced by another backup software product [redacted].

In accordance with CIP-010-2 R1.2, authorization for this change was received on 4/13/2017, and in accordance with CIP-010-2 R1.4, pre- and post-change security controls checks were completed on 4/14/2017 and 4/26/2017, respectively. The root cause of this issue was a failure to properly document changes to [redacted] [redacted] servers within 30 days of the software removal in accordance with the [redacted], which instructs business unit personnel to "update the baseline configuration documentation such that the date of update is within 30 calendar days of the implementation date recorded in the change documentation."
Summary:
Determining the extent-of-condition for all of these issues was done by completing a comprehensive baseline documentation review as part of the mitigation milestone (14) by 6/29/2017 as part of oper [redacted] Scope Expansion of [redacted]). To prevent future recurrence of this issue, targeted training with [redacted] Tech Org personnel responsible for these change management and baseline documentation updates was conducted as part of the mitigation milestone #15 by 6/29/2017. Additionally, to prevent future recurrence, [redacted] Tech Org has implemented new technical controls to perform a line by line comparison between the baseline documentation software inventory and software actually installed on systems, and a comparison between the baseline configuration ports and services whitelist and the listening ports and services on systems.

There was no known harm that occurred as a result of these issues.

Attachments ()

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

For the first issue [redacted] this was considered a documenta[redacted] failed to include a necessary and enab[redacted]e [redacted]or [redacted] servers i[redacted] ESPs that were u[redacted] loggers for each ESP ([redacted] ESPs were in place at t[redacted] this issue). Th[redacted] to forward ESP devic[redacted]r [redacted] server that serves as a log aggregat[redacted] used t[redacted]efine policies and alerts for [redacted]

• On each of the [redacted] servers, a host-based firewall had also been configured in accordance with [redacted]1 to allow services to use port [redacted] logging. [redacted]

• During the extent of condition review as part of milest[redacted]2 of this mitigation plan, [redacted] also d[redacted]overed that the nec[redacted]d [redacted] was also missing in the spreadsheet documentation – for the same [redacted] devices. The host-based firewall had [redacted]red in accordance with CIP-007-6

R1 to allow serv[redacted]nd whitelisting using the Tra[redacted] product – it was only the spreadsheet used for CIP-010-2 R1 to document the necessary p[redacted]se[redacted] was inaccurate. [redacted]

[redacted]etermine the exte[redacted]on, the [redacted] group performed a reconcilia[redacted] base[redacted] against cyber asset configurations that covered all operating co[redacted]hy medium impact S[redacted]-scope" CIP cyber assets, and completed this [redacted]w on 10/6/2016 as part of [redacted] (this was prior to the on-site portion of the 2016 SERC CIP au[redacted]).

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

• A[redacted]rt of the closure package that was s[redacted]with this self-report mitigatior[redacted]hat in addition to the original [redacted] that was missing in the baseline sp[redacted] was also found to be missing as noted on line 154. [redacted]

• T[redacted]losure package states: [redacted] As noted on F[redacted]on of this milestone review, one [redacted]authorized logical network accessible [redacted] was discovered to no[redacted] included in the previous bas[redacted]entation. [redacted] The "C[redacted]g" tab of thi[redacted]sheet sh[redacted]he [redacted] Transmi[redacted]seline [redacted]e subseque[redacted] discovered open [redacted]lude Supervisor Approval (see Milestone 3).

• The EOC review for this issue did not include a review of EMS CIP cyber asset baseline document[redacted]1/2016 a [redacted] that allows th[redacted]ntain automate[redacted] line documentation and evidence as per CIP-010-2 R1. Therefore, it was assessed that the possibility of the potential for the same [redacted]ntation error' in EMS did not exist.

Th[redacted] arent root-cause of this issue[redacted]a human perform[redacted]cluded in the baseline documentation due to a transcription error. Both po[redacted]nally included in baseline do[redacted]station devices, however, prior to July 1, [redacted] decided to create separate baseline do[redacted]ntation for each [redacted]umen[redacted]g the pr[redacted]s of transferring baseline documentation fro[redacted]ocument into 5 separate documents, these two [redacted]errant [redacted]ncluded. To prevent future recurrence [redacted]sue, a secondary Supervisor review of ar[redacted]o the Trans[redacted]fications was implemented by October 31, 20[redacted]see mit[redacted] step #3). [redacted]

[redacted] discovered this issue while responding to a Level 2 Data Request in preparation for [redacted] SERC CIP compliance audit. In preparing a response to the Level 2 Data Request, [redacted] personnel discovered that the [redacted] Transmission baseline documentation inadvertently failed to list one (1) authorized enabled port. The second port was discovered as a result of mitigation activities related to this self-report, as described in response to question #2 above.

For the second issue [redacted] involving the sampled EMS device baseline, during the 2016 SERC CIP Audit, there was a correction in the documentation for the ports and services whitelist used to demonstrate compliance with CIP-007-6 R1.1 for Cyber Asset [redacted]" Originally, the ports and services whitelist included an ephemeral port range used by [redacted] While under discussion with the SERC Audit Team, the range was narrowed and updated to reflect the more specific ephemeral port range used by these [redacted] devices based on additional discussions with [redacted] and [redacted] support [redacted] It was determined that while collecting the unique ports and services for the [redacted] EMS included the full ephemeral range (not network accessible ports) for EMS support purposes only. After reviewing this information, the SERC Audit Team removed their concern and concluded the on-site audit week with no noted potential violations. In the SERC Audit Final Report, this concern returned in the form of an audit finding and RFI, stating that an overly broad range was included in the CIP-010-2 R1.1 baseline for logical network accessible ports (R1.1.4). The port range in question for EMS was depicted in the baseline documentation as the "ephemeral port range" used by the [redacted] devices. Ephemeral ports are not considered logical network accessible ports. The below information clarifies EMS's use of ports and services whitelists and the inclusion of ephemeral ports, which they believe is exceeding the requirements of the standard.

EMS Whitelists (Ports & Services)

NERC CIP-007-6 R1.1: Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.

Measure: Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. [1]

EMS utilizes discussions with impacted key stakeholders (including Subject Matter Experts) to capture business needs, information from equipment vendors and integrators, and system configuration information to establish the necessary ports and services whitelists as per CIP-007-6 R1.1. [2]

EMS Baselines

NERC CIP-010-2 R1.1 Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.4. Any logical network accessible ports;

Measure: A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group. [3]

EMS subject matter experts create a baseline for each EMS device that has been commissioned per the EMS Commissioning Equipment Work Practice. In Section 4.1.1, Step 1 of the EMS [redacted] Work Practice, EMS utilizes the [redacted] to capture the current configuration state of each device, and to confirm the documented elements of the baseline configuration match the current configuration state of the device. This includes operating system/firmware, commercial software, custom software, logical network accessible ports, and Security Patches. [4] [5]

EMS has implemented the capability for the [redacted] tool to monitor, identify, document and report when a device experiences any deviations from the baseline configuration (operating system/firmware, commercial software, custom software, logical network accessible ports, and Security Patches). [5] EMS business processes include use of these reports in correlating the changes to authorized change records and to detect any potential unauthorized changes.

Ephemeral Ports

Ephemeral ports are short-lived ports automatically allocated from a predefined range within an operating system's IP stack. These ports are TCP or UDP protocol ports assigned for outbound (Client side) communication to other devices (Server), which is known as Client – Server communication. For certain protocols, ephemeral ports may be used to hand off an established session, but only after initial communication is established to the well-known network accessible port for a device. At no time is the Ephemeral port accessible for any other communication.

Examples of this usage include continuation of communication for File Transfer Protocol (FTP) or Remote Procedure Call (RPC). These allocations are temporary and valid only for the duration of the communication session. After the communication session is complete and the operating system defined timeout has occurred, the port is automatically re-claimed for future reuse. [6]

Consistent with the definition provided above, ephemeral ports are not considered network accessible – but are used to facilitate client-initiated, short-lived, unique communication paths. As a result, ephemeral ports are not considered part of the CIP-010-2 R1.1.4 baseline requirements.

EMS Rationale for Enumerating Ephemeral Port Ranges in CIP-007-6 Ports and Services "Whitelists"

EMS maintains ports and services "whitelists" in accordance with CIP-007-6 R1.1 and references these whitelists during security controls testing, vulnerability assessments, and commissioning tasks. [2]

During these activities, EMS personnel and tools compare output from commands including [redacted] with the ports and services whitelists. [redacted] command output returns a list of all active logical network accessible ports. However, [redacted] also returns some short-lived ephemeral ports that are active at the time that the command is executed.

If EMS had performed external network scans for open ports, using tools like [redacted] only network accessible ports would be returned. No ephemeral ports would be visible in the external network scan.

Based on EMS's selected method of information collection, and for EMS support purposes only, ephemeral ports are included in the ports and services whitelists in order to ease the burden of comparison between command output and each device's appropriate "whitelist".

As part of the [redacted] CIP Procedures Manual, [redacted] has a Cyber System Management procedure [redacted] that addresses the lifecycle of applicable CIP Cyber Systems and the development of baseline configuration documentation. This procedure takes all of the various requirements and tasks associated with the technical management of cyber assets or cyber systems (CIP-007 requirements and the baseline configuration and vulnerability assessment portions of CIP-010) and organizes these tasks by the lifecycle stage of the applicable system for ease of use by support personnel. It includes the steps to follow for planning for a new CIP Cyber System (Section 4.1), commissioning a new CIP Cyber Systems (Section 4.2), maintaining existing CIP Cyber Systems including tasks performed at varying periodicity throughout the system's lifetime (Section 4.3), and decommissioning CIP Cyber Systems (Section 4.4).

CIP-010-2, Requirement 1 Part 1.1 is addressed in the procedure as follows:

• Section 4.1.3 to 4.1.6, Planning stage: requires the creation of a new baseline configuration including OS/firmware, application software, custom software, logical network accessible ports, and applied security patches during the planning stage.

• Section 4.2, Commissioning stage: Steps 1, 2, and 5 require the validation of the ports and services and security patch levels against those documented in the baseline configuration prior to commissioning.

[redacted] EMS follows the [redacted] Cyber System Management procedure [redacted] as identified above and the EMS Configuration and Change Management Work Practice to ensure the baseline configurations of the EMS BES Cyber Systems and their associated EACMS and PCAs are created, updated, and managed.

CIP-010-2, R1 Part 1.1 is addressed in the work practice as follows:

• Section 4.1.1, Step 1 - specifies the process of establishing an initial baseline configuration for operating system/firmware, commercial software, custom software, logical network accessible ports and security patches.

[redacted] Transmission Substations adheres to the [redacted] procedure and the (CIP-010-2) Baseline Configuration Change Management Work Practice for development of baseline configurations. For Transmission Substations, baseline configurations are grouped by manufacturer and model, and then additional baseline configurations are created for models with different baseline items (ex. [redacted]).

Sections 4.0-4.6 of the (CIP-010-2) Baseline Configuration Change Management Work Practice details the location of the [redacted] Transmission Baseline Configurations spreadsheet and the information sources for populating the spreadsheet with new baseline configurations.

These issues were not discovered through a formal internal controls process.

Additionally, the following provides information related to the previously submitted SERC [redacted] issues.

The original issue was discovered by [redacted] Tech Org personnel by conducting post-change security controls verifications. When updates are made to CIP cyber assets, Tech Org personnel perform a CIP Cyber System - Cyber Security Controls Verification. One of the verifications is to review the "Necessary Ports and Services Enabled". The issue was discovered during the cyber control verification after an update to a CIP cyber asset.

Detection of the issues filed under Scope Expansion #1 on 5/18/2017 and Scope Expansion #2 on 9/15/2017 were discovered via either a chance event during the performance of pre- and post-change security controls checks, or as part of extent-of-condition reviews and mitigating previous issues. 5 of the 11 issues were found as part of the pre-security control check, 5 were found during baseline verifications performed mitigating a previously reported issue, and 1 was found in preparation for the annual BES Cyber System and associated Cyber Asset review and update.
For the pre-security controls check, prior to any change which would impact a baseline component, if the change has the potential to impact a defined security control, there are steps in place to follow (as documented in CIP-IT-022 – Configuration Change Management work practice), in order to verify that the Cyber Security Control is in place and that it is configured in accordance to procedure and/or documented baseline evidence. Some checks are manual, and some are scripted. The frequency in which these checks occur are as needed and prior to any change which is made that deviates from the existing baseline configuration. The manual check process has been in use since prior to the July 1, 2016 commission date of all [redacted] Technology Organization supported CIP cyber assets. Some scripted controls checks were developed prior to the July 1, 2016 commission date and in use at that time, however others have been developed periodically since the commission date until present time.

The [redacted] Tech Org determined the extent-of-condition for the original issue through mitigation step 2, which provided Tech Org will perform a review of all [redacted] cyber system baseline documentation and verify all are up to date and accurate, and include any installs, upgrades, or updates implemented prior to July 1, 2016. Tech Org is responsible for managing [redacted] EACMS/PACS servers and [redacted] PACS monitoring workstations that include the following systems: [redacted] The initial reviews were expected to be completed on November 18, 2016; however, additional instances of potential non-compliance were discovered as of January 5, 2017 and February 27, 2017. This resulted in the filing of a scope expansion to the existing self-report ([redacted] where [redacted] IT committed to the performance of another review of the baseline documentation for the above listed assets to confirm accuracy as of 6/29/2017. Execution of these new milestones revealed additional instances of potential non-compliance with CIP-010-2 R1 as of 6/10/2017, which was filed on the portal on 9/15/2017 as Scope Expansion #2 to 16-2527.
In total, for all 11 issues combined above, [redacted] of [redacted] servers/workstations were impacted, and [redacted] out of [redacted] PACS controller panel assets were impacted.
[redacted]

For these impacted cyber assets, their impact classification/association and purpose is as follows:
- [redacted] (EACMS for Medium Impact BCS) – [redacted]
- [redacted] (EACMS for Medium Impact BCS) - Security Monitoring Application used to meet CIP-007 R4 logging and monitoring requirements for all High and Medium Impact PACS and EACMS' supported by [redacted] Technology Organization
- [redacted] Servers (EACMS for Medium Impact BCS) – Databases for the [redacted] architecture which is used as a centralized means for communicating with Intelligent Electronic Devices (IEDs) that are located within transmission substations.
- PACS [redacted] Servers, Workstations, Controller Panels (PACS for High Impact BCS) – Card Access and Badging control software controlling physical access to PSP's.

The total durations of non-compliance for each issue is as follows:
- Issue 1 [redacted]
- Issue 2 [redacted]
- Issue 3 [redacted]
- Issue 4 [redacted]
- Issue 5 [redacted]
- Issue 6 [redacted]
- Issue 7 [redacted]
- Issue 8 [redacted]
- Issue 9 [redacted]
- Issue 10 [redacted]
- Issue 11 [redacted]
- All of these issues occurred following the CIP V5 effective date of 7/1/2016 and the latest mitigation date of these issues combined was 6/22/2017 – 11 months, 22 days.

The following provides the duration dates that are applicable to these issues and why these dates are used:
- Issue 1 ([redacted]) – 07/01/2016 (the date of asset commissioning) through 08/25/2017 (the date the Ports/Service Whitelist was updated to include the missing port information/business justification)
- Issue 2 ([redacted]) – 08/04/2016 (the date the patches were installed) through 09/8/2016 (the date the Security Patch Log component of the baseline was updated to include the missing security patch information)
- Issue 3 ([redacted]) – 08/15/2016 (the date the [redacted] software upgrade was installed) through 09/14/2016 (the date the post cyber security controls verification was performed on each of the [redacted] severs)
- Issue 4 ([redacted] on PACS) – 08/18/2016 (the first date the [redacted] software upgrade was performed on any of the impacted assets) through 10/7/2016 (the date the Software Inventory component of the baseline was updated to include the missing software upgrade information)
- Issue 5 ([redacted] and [redacted] on [redacted]t [redacted] – 07/01/2016 (the date of asset commissioning) through 01/05/2017 (the date the Software Inventory component of the baseline was updated to include the missing software information)
- Issue 6 (PACS panels) – 07/01/2016 (the effective compliance date for CIP-010 R1) through 03/09/2017 (the date the Cyber System Inventory was updated to include the [redacted] new assets and the same date the Firmware Inventory component of the baseline was updated to include the missing firmware upgrade information for the other [redacted] existing panel assets).
- Issue 7 (Ports & Services) – 07/01/2016 (the date of commissioning these [redacted] PACS assets) through 6/21/2017 (the date the Ports & Services component of the baseline documentation was updated to include the port & service information)
- Issue 8 ([redacted] Agent) – 07/01/2016 (the date of commissioning these [redacted] PACS assets) through 6/22/2017 (the date the Software Inventory component of the baseline documentation was updated to include the missing [redacted] software information)
- Issue 9 ([redacted]) – 4/22/2017 (the date [redacted] upgrade was installed on these [redacted] PACS assets) through 6/22/2017 (the date the Software Inventory component of the baseline documentation was updated to include the current [redacted] software version)
- Issue 10 [redacted]) – 2/22/2017 (the date [redacted] was installed on [redacted] PACS workstation assets) through 6/22/2017 (the date the [redacted] software was uninstalled on the [redacted] PACS assets. Within the same timeframe for this issue, [redacted] software was also inadvertently installed on 5/18/2017, detected on 6/14/2017, and uninstalled on 6/15/2017 for four other PACS workstation assets – making [redacted] PACS workstation assets in total).
- Issue 11 ([redacted]) – 4/18/2017 (the date [redacted] was uninstalled) through 5/18/2017 (the 30 days allowed to complete baseline documentation updates based on a change). Baseline documentation updates were completed, however, on 6/14/2017, which was 27 days after 5/18/2017.

Programmatically, the apparent root cause of these issues has been a lack of oversight and attention-to-detail with regard to manual control processes and properly excluding assets from enterprise wide deployments. Continuous process improvement, management emphasis, and streamlined technical controls being implemented should greatly help reduce recurrence of these issues.
The [redacted] Technology Organization has well documented processes for corporate/enterprise asset management, as well as CIP-specific processes and work practices for managing CIP cyber systems. However, a contributing factor to reoccurrence of these issues has been lack of accountability and ownership of understanding the documented procedures and work practices in this organization. In addition, resource constraints in this organization have been an ongoing contributing factor for properly managing CIP assets.

Prior to the effective date of 7/1/2016 of Version 5 of the CIP Standards, the [redacted] Technology Organization had a minimum number of assets they managed that were in-scope of V3 of the CIP standards. Those assets at the time were network components that fell under the EMS organization and the overall [redacted] CIP Compliance Program. EMS maintained oversight and monitoring of compliance for those network assets.

In the lead up to the effective date of CIP V5, however, with the scope of Substation assets increasing, it was recognized that access control (EACMS) assets supporting the Substations would need to be moved off of the corporate networks and into their own dedicated domain. The [redacted] Technology Organization took on the responsibility of establishing this dedicated domain, along with the implementation of supporting EACMS assets, such as new domain controllers, [redacted] infrastructure, virtual infrastructure hosting Intermediate Systems, etc. In addition, the Tech Org also implemented security event monitoring systems such as [redacted] on this dedicated domain for supporting CIP-007 R4 for the Substation CIP assets. This included responsibility under CIP-004, CIP-005, CIP-007, CIP-010, and CIP-011 for [redacted] physical/virtual Cyber Assets, and [redacted] PACS controller panels. The personnel involved in establishing this new domain and implementing these new systems did not have past experience with the CIP Standards and have been faced with learning curve challenges, as well as resource constraints.

To reduce the potential possibility of continued issues going forward, [redacted] Tech Org is evaluating the possibility of adding a peer review for all NERC CIP Change Cases to promote adherence with the various Change Management requirements prior to the closure of a change management window. This additional review will help ensure that approvals and pre-security controls checks are performed prior to the actual change, and will also help ensure that the post-security controls checks and updates to baseline documentation is validated as being complete prior to the closure of the change case. Failure of any of the requirements will result in the change case being denied until all requirements are fulfilled. Furthermore, any failures will be communicated to management for accountability and reinforcement of procedure.

To enhance the Tech Org Education model, the development of additional training delivery methods are currently underway. This will include a Tech Org [redacted] channel with instructional videos, as well as additional [redacted] training modules where employees can engage in a variety of more targeted learning sessions. Also, additional resources have been approved, acquired, and added to the priority areas to assist in the day to day management of the Tech Org CIP environment. Below is a description of root cause analysis for each issue:

• Issue 1 [redacted] Ports) – A baseline documentation error where the application owner failed to update the Ports/Services Whitelist, which is a manual process, within 30 days of the change.
• Issue 2 (Patches on PACS) – The patches were being delivered to the rest of the [redacted] via [redacted] but were inadvertently added to a [redacted] Security Patch Deployment "roll-up" group which contained the 1 PACS server. This server should have been excluded from this group by he person deploying patches, but was not.
• Issue 3 ([redacted]) – The [redacted] EACMS servers were part of an enterprise managed group of all [redacted] IT-managed [redacted] servers. The servers should have been excluded from this group, but were inadvertently left in and therefore the [redacted] software upgrade was deployed to these [redacted] servers at the same time it was deployed to the rest of the [redacted] enterprise.
• Issue 4 ([redacted]) – The [redacted] software upgrade from version [redacted] on [redacted] PACS assets was a result of an enterprise deployment pushed out on the corporate [redacted] domain. This deployment was unintended and occurred because the Active Directory Software [redacted] for PACS [redacted] servers and workstations leveraged the same [redacted] package used for the enterprise [redacted] deployment. This software was later deemed to not be needed on PACS assets and was uninstalled.
• Issue 5 ([redacted] – A baseline documentation error where the application owner failed to list these two software components on the Software Inventory baseline, which is a manual process.
• Issue 6 (PACS panels) – A failure on the part of the [redacted] and personnel within the [redacted] Corporate Security groups to properly coordinate and document changes to PACS controller panels at the time of the change, which is a manual process.
• Issue 7 (Ports & Services) – In confirming accurate baseline documentation as part of the original mitigation plan of this issue, local port scans of [redacted] PACS monitoring workstations revealed additional ports enabled on these devices. It was determined that the port scanning method previously used failed to recognize these ports as enabled because the original script prevented the identification of the higher range UDP ports, and the [redacted] scan being performed remotely was masking the identified ports. All of the ports were deemed needed, therefore baseline documentation was updated to include them.
• Issue 8 [redacted]) – In confirming accurate baseline documentation as part of the original mitigation plan of this issue, installed software inventories of [redacted] PACS monitoring workstations revealed the [redacted] software installed on these devices for [redacted] as of 7/1/2016 was not included in previous baseline documentation. The analyst responsible for the software inventory component of the baseline documentation overlooked it given the security nature of the software agent.
• Issue 9 [redacted]) – This was a baseline documentation error where the application owner failed to save the updated Software Inventory baseline documentation in the proper storage location, which is a manual process. Baseline documentation updates were made at the time of the change, however, the spreadsheet could not be located after the fact.
• Issue 10 [redacted]) – This issue involved inadvertent installation of software outside the change management process. In both instances, the analyst deploying the software should have excluded the PACS workstations from the proper groups, but they were inadvertently left in and therefore the software was deployed to these PACS workstation assets at the same time it was deployed to the rest of the [redacted] workstations. The number of analysts with the capability to use [redacted] to deploy enterprise updates has been reduced and personnel were re-trained on proper software deployments and properly excluding/including PACS workstation assets, when needed.
• Issue 11 ([redacted]) – This issue involved a baseline documentation error where the application owner failed to completely update the Software Inventory baseline documentation, which is a manual process. Baseline documentation updates were made at the time of the change, however, the row in the baseline spreadsheet listing the [redacted] software was only partially lined-out and still showed an installation "Active" status in one column of the row, which was causing discrepancies in scripted baseline comparisons.

As part of the [redacted] CIP Procedures Manual, [redacted] has implemented the [redacted], Cyber System Management procedure to address CIP-010-2 R1. [redacted] business units develop baseline configurations in accordance with [redacted] NERC CIP procedure [redacted], Cyber System Management. [redacted] addresses the lifecycle of applicable CIP Cyber Systems. This procedure takes all of the various requirements associated with the technical management of cyber assets or cyber systems (including the baseline configuration requirements of CIP-010) and organizes these tasks by the lifecycle stage of the applicable system for ease of use by support personnel. It includes the steps to follow for planning for a new CIP Cyber System (Section 4.1), commissioning a new CIP Cyber Systems (Section 4.2), maintaining existing CIP Cyber Systems including tasks performed at varying periodicity throughout the system's lifetime (Section 4.3), and decommissioning CIP Cyber Systems (Section 4.4).
• Planning stage - Section 4.1, Steps 3 through 8 require the creation of a new baseline configuration including OS/firmware, application software, custom software, logical network accessible ports, and applied security patches during the planning stage.
• Commissioning stage - Section 4.2, Steps 1,2, and 5 require the validation of the ports and services and security patch levels against those documented in the baseline configuration prior to commissioning.

Additionally, [redacted] Cyber System Management Procedure, Section 4.1.5 – 4.1.8 instructs:
4.1.5 Needs Assessment
Determine any needed Ports and Services. This information can be determined using one or more of the following methods:
• Information from equipment or software vendors and integrators.
• System or network scans.
• System configuration information.

If the CIP Cyber System has no provision for disabling or restricting Ports and Services on the CIP Cyber System, then those Ports and Services that are open are deemed needed.

4.1.6 Ports and Services Whitelists
Select an existing Ports and Services whitelist that matches the CIP Cyber System Ports and Services configuration exactly or produce a new Ports and Services whitelist. See 5.3, Evidence for Each Ports and Services Whitelist, for required attributes for the whitelist.

4.1.7 Disable Unnecessary Parts and/or Services
Disable the unnecessary ports, associated services, or stand-alone local services. Disabling the port can be accomplished by disabling the listening service or blocking the port at the operating system level by using a host-based firewall rule. If an unnecessary port or service cannot be disabled, see [redacted] to submit and request approval of a TFE.

4.1.8 Baseline Configuration
Determine if the CIP Cyber System baseline configuration matches an existing baseline configuration, and if so, document the inclusion of the CIP Cyber System into the baseline configuration group. If not, document the new baseline configuration. See section 5.2, Evidence for Each Baseline Configuration.

The [redacted] Technology Organization also maintains the following business unit specific work practice(s) which dictate the necessary steps to address each of the processes described above which had failures.
• [redacted] - Ports and Services on [redacted] and [redacted]
o This work practice provides steps to ensure that only those ports and services required for normal and emergency operations are enabled, and documented on the Baseline documentation for "Ports and Services Whitelist" on applicable Cyber Assets. Section 4.1 (including sub-sections 4.1.1 – 4.1.6), describes the process for collecting ports/services on the various in scope CIP assets. Section 4.2 provides reference to the work practice which covers properly updating the baseline files ([redacted] -Baseline Creation and Modification).
• [redacted] Baseline Creation and Modification
o This work practice describes steps to document the attributes needed to create and update a Baseline Configuration file for CIP Cyber Systems. Section 4.1 and it's sub-components describes the process for creating a baseline, while section 4.2 and its sub-components describes updating and maintaining baseline documentation.
• [redacted] - Configuration Change Management
o This work practice document the steps required to submit the Change Management and references the above procedures which need to be executed to generate the appropriate evidence for the corresponding baseline configuration change. Section 4.3 and its sub-components describe the Remedy Change Mgmt process, including the Implementation plan and the steps necessary in creating the actual change case. Section 4.4 describes the need for change management for any changes to baseline components of the in-scope CIP Cyber Systems. Section 4.5 describes the change management approval process. Section 4.6 describes the Cyber Security Controls Pre-Verification process. Section 4.8 describes the Cyber Security Controls Post-Verification process. Section 4.9 and its sub-components provides reference to the work practice which covers properly updating the baseline files ([redacted] -Baseline Creation and Modification).
• [redacted] - Commissioning New Cyber Assets
o This work practice is an overarching document to assist with commissioning a new Cyber Asset. This document documents the process from when asset hardware order is received until it is completely setup. Each requirement is outlined and references the appropriate work practice, which details each requirement process as well as walking through the collection of the required evidence, until the new CIP Cyber Asset has been commissioned to the production environment.

? Section 4.1.4 references the [redacted] - Cyber Systems Inventory work practice used for creating/maintaining a Cyber System Inventory for all CIP Cyber assets.
? Section 4.1.5 describes the process for device categorization within the Cyber System Inventory
? Section 4.1.6 references the [redacted] - OS Firmware and Appl Software Installed work practice used for documenting the installed OS/Firmware and Software baseline components.
? Section 4.1.8 references the [redacted] - Ports and Services on Windows and Linux work practice used for documenting the Ports and Services Whitelist baseline component
? Sections 4.1.9 and 4.1.10 references [redacted] - Monthly Deployment of Security Patch Updates work practice used for documenting the Security Patches baseline component
? Section 4.1.11 references [redacted] Baseline Creation and Modification work practice used for documenting all baseline components

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

• [redacted] - Cyber Systems Inventory
o This work practice describes steps to document the attributes for each in-scope CIP Cyber System for IT managed servers and appliances. Section 4.0 and all sub-components describe the process for documenting all necessary components of the Cyber System Inventory.
• [redacted] - OS Firmware and Appl Software Installed
o This work practice describes steps to document the Operating System (OS), Firmware, and Application Software installed components of the Baseline Configuration file for CIP Cyber Systems. Section 4.1 describes the process for adding and managing the OS/Firmware and software component of the baseline. Section 4.2 references [redacted] - Baseline Creation and Modification work practice used for documenting all baseline components
• [redacted] Monthly Deployment of Security Patch Updates
o This procedure outlines roles, responsibilities, and processes for the monthly deployment of security updates to in scope CIP Cyber Systems to document the evidence required for the baseline of those systems. Section 4.1 describes the process for evaluating the security patch source every 35 days. Section 4.2 describes the process for determining applicability of a security patch. Section 4.5 describes the process for installing security patches. Section 4.6 describes the process for updating the Security Patch Log baseline documentation component. Section 4.10 references [redacted] Baseline Creation and Modification work practice used for documenting all baseline components

These issues were not discovered through a formal internal controls process.

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:

Description of Mit[redacted]vities:
[redacted] Transmiss[redacted]clude the open [redacted] 9/6/16)
2. Review [redacted] Transmission baseli[redacted]o [redacted]all authorized logical network access [redacted] are in[redacted]ded. (Completed 10/6/16)
[redacted]ondary Supervisor review [redacted]anges to [redacted]sion baseline d[redacted]ation and business justifications to ensure all ports enabled a[redacted] required for opera[redacted]ciated baseline documentation. Supervisory review shall be captured in the b[redacted]nge log. (Completed 10/26/16)
[redacted]
Details to Prevent Recurrence: Execution of the above n[redacted]tion steps will correct the [redacted]ue and [redacted]event future recurre[redacted]
Additionally, the [redacted]previously submitted SERC [redacted]sues.
[redacted] Technology Orga[redacted]mpleted [redacted] following:
1) [redacted] Tech Org updated [redacted] Host ports and services whitelist as part of th[redacted]eline documentation to include the open [redacted] as it is required for [redacted] Completed 8/25/2016
2) [redacted] Tech Org performed a review of all [redacted] CIP cyber system baseline [redacted]accurate, and included any ins[redacted] upgrades, or updates implemented [redacted] Completed 11/18/2016
3) [redacted] Tech Org conducted a [redacted] addressing C[redacted]partment personnel on updating [redacted]ocumentation within the required time [redacted] Completed 12/6/2016 [redacted]
[redacted]entatior [redacted] that they ha[redacted]wed and [redacted]d th[redacted]dural step[redacted]ee to [redacted] 2/6/2016 [redacted]
[redacted]o issue SERC [redacted] the following m[redacted]umber 5, which is an extension of the original self-report and the four milestones contained therein.
5) [redacted] Tech Org removed all EACMS [redacted] servers from the [redacted] enterprise management containers, changed them to the All EACMS [redacted], and moved them to a new [redacted] container for future backup agent deploy[redacted]t [redacted]Completed 8/26/2016
6) [redacted] Tech Org update[redacted]mplete[redacted]
7) [redacted] Tech Org excluded all CIP PACS systems [redacted]roll-up" patch deployment collections (including [redacted], [redacted] and [redacted] enterprise deployment collections) and [redacted]em to collections for all future targeted C[redacted]atch deplo[redacted]
8) [redacted] Tech [redacted]dated the PACS baseline documentation to include the [redacted] software upgrade. [redacted]pleted 10/7/2016
9) [redacted] Tech Org updated the PACS baseline documentation to include the PACS controller panel firmware upgrades and PACS controller replacements. Completed 3/23/2017
10) [redacted] Ops Compliance conducted a review and oversight session with Executives over the [redacted] Technology Organization to emphasize the importance of compliance with the CIP Standards. Completed 4/25/2017
11) [redacted] Tech Org reviewed [redacted] IT Work Practices applicable to CIP-010-2 R1 for areas where additional instruction was added to help prevent re-occurrences. Completed by 6/2/2017
12) [redacted] Tech Org implemented organizational changes to the [redacted] structure to provide additional personnel responsible for CIP compliance tasks to prevent future issues of the same or similar requirements. Completed by 6/15/2017
13) [redacted] Tech Org reviewed each configuration management tool to ensure CIP assets were not included into any enterprise rollup groups to prevent unintentional deployment of updates outside the CIP Change Management process where possible. Completed by 6/29/2017
14) [redacted] Tech Org performed a review of all [redacted] and PACS baseline documentation, and verified all are up to date and accurate. Completed by 6/29/2017
15) [redacted] Tech Org conducted a review / training session with departmental personnel and management on applicable changes to [redacted] IT Work Practices addressing CIP-010-2 R1. Completed by 6/22/2017
16) [redacted] Tech Org Application Support and the [redacted] conducted a review / retraining session with PACS system administrators on he process for replacing controller panel hardware. Completed by 6/27/2017
17) [redacted] Operations Compliance completed a comprehensive review of all required evidence associated with this mitigation plan and prepare and submitted a closure packet for SERC review of these potential violations. Completed by 7/18/2017

As part of Scope Expansion #2 to issue SERC [redacted], the following milestones start at number 18, which is an extension of the original self-report and scope expansion #1 and the seventeen milestones contained therein. A consolidated closure package including evidence for all 24 milestones will be provided to SERC upon completion of the last milestone.
18 [redacted] Tech Org implemented technical controls to perform a line by line comparison between the baseline documentation software inventory and the software actually installed on the systems. Completed 6/9/2017
19 [redacted] Tech Org developed and deployed technical controls to perform a comparison between the baseline configuration ports and services whitelist and the listening ports and services derived from the output of the [redacted] command. Completed 6/9/2017
20) [redacted] Tech Org updated the PACS ports and services whitelist as part of the baseline documentation to include the [redacted] range) associated with the necessary [redacted] service. Completed 6/21/2017
21 [redacted] Tech Org updated the PACS Workstations SW inventory as part of the baseline documentation to include the upgraded [redacted] version and the [redacted]. Completed 6/22/2017
22) [redacted] Tech Org verified the [redacted] software was removed from the PACS Workstations. Completed 6/22/2017
23) [redacted] Tech Org verified the [redacted] Antivirus software was removed from the PACS Worksta ions. Completed 6/22/2017
24) [redacted] Tech Org implemented changes to the [redacted] to limit the number of administrator's ability to update CIP Assets. Completed 7/18/2017

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:

7/18/2017

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

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

Update Baseline Docs

Milestone Completed (Due: 9/6/2016 and Completed 9/6/2016)

Update [redacted] Transmission baseline documentation to include the open port.

Review All Other Baseline Docs

Milestone Completed (Due: 10/14/2016 and Completed 10/6/2016)

Review [redacted] Transmission baseline documentation to ensure all authorized logical network accessible ports are included.

Supervisor Review Process

Milestone Completed (Due: 10/31/2016 and Completed 10/26/2016)

Implement a secondary Supervisor review of any changes to the Transmission baseline documentation and business justifications to ensure all ports enabled and required for operations are included in the associated baseline documentation. Supervisory review shall be captured in the baseline change log.

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):

(i) There are no k[redacted]ional risks or impacts to the BPS w[redacted]s mitigation plan are being completed[redacted] risks to the reli[redacted]S as part of this mitigatio[redacted]plan. [redacted] assesses the first issue [redacted]posed a r[redacted]l risk, and not a[redacted] or substantial risk to the reliability of the bulk electric system [redacted]e ports in question [redacted]mentation were enabled to send device logs from non-windows systems to an [redacted] aggregator. The [redacted] issue is limited to a doc[redacted]entation error. Although th[redacted]ort information was errantly omitted in the Transmission Substation's baseline documentation used for CIP-010-2 R1.1, the port and its business justif[redacted]n were included in the C[redacted]005-5 [redacted]3 firewall rulesets. [redacted] T[redacted]ssion was aware of the ports in question and had a valid business justif[redacted]/enabled. A thorough review of the [redacted] Transmission baselines determined that [redacted]e properly documented. [redacted]

[redacted]the second issue [redacted]elated t[redacted]MS baseline documentation, [redacted] asse[redacted]ed a minimal actual risk, and not a serious or substantial risk to [redacted]eliability of the bulk [redacted]m. At the time of forming the whitelists for the [redacted] devices, there was nothing in vendor do[redacted]ion that indicated a "[redacted] broad" ephemeral port range than the potential range of [redacted]wever, in this case, EMS did not have any indication at the time that the devices never used the full ran[redacted]pecified. The spreadsheet containe[redacted]hat was neither observed on [redacted]st vendor documentation. [redacted]
• After the range was questioned by [redacted] audit data request, EMS conducted additional interrogation of the [redacted] devices on October 4th, 2016 and de[redacted]ed that the range shou[redacted]-007 R1 EMS [redacted]. Additionally, EMS reached out to [redacted]upport to request that they confirm the [redacted]ral port range for the [redacted] devices. As indicated in the [redacted]-2-R1 PV EMS Email from [redacted] vendor [redacted]tation, and [redacted] support [redacted] a [redacted]ainst the [redacted] to request [redacted]ating the table wh[redacted]ts." The evidence provided shows vendor verification and documentation of the ephemeral port range that was previously unavailable, but was being added as [redacted]sers. [redacted]eral ports are [redacted]or device functi[redacted]le to many types of applications on an as-needed basis. As they are required for device function, we expect to see them when scanning [redacted]tomated tools. The justification for ephemeral ports is the same, regardless of the size of the range or the [redacted] of device. In the case of the [redacted] devices, a local fi[redacted]l ports providing a service would not be externally visible to a network [redacted]xternal user, but would be v[redacted]access for scanning/discovery via netsta[redacted]h[redacted]s also supported through the evi[redacted]e provided in the [redacted]Octob[redacted]16. [redacted]

[redacted]ally, the following provides information rel[redacted]reviously s[redacted] issues. [redacted]
Given the repeat nature of these issues and their potential impact to authentication and Interactive Remote Access to Transmission Substation medium impact BES Cyber Systems [redacted] assesses these issues posed a moderate risk, and not a serious or substantial risk to the reliability of the bulk electric system. Potential risk could include the introduction of unknown vulnerabilities susceptible to exploitation by not following documented processes, by not maintaining proper documentation of baseline configurations, by not ensuring proper authorization of changes to cyber assets, and by not verifying security controls after implementing a change or upgrade. Failure to follow documented processes could have led to the introduction of vulnerabilities without detection at the time that could have potentially made EACMS assets unavailable or degraded if exploited.

Although many of these issues are documentation errors, other issues herein stem from the preemptive installation of security patches and software upgrades where CIP assets were susceptible to enterprise deployment policies. The patches and software in question were applicable, required, and the installation of which made those CIP assets more secure. The [redacted] Tech Org has strong procedural controls built into their work practices and documentation; however, these issues identify the need for additional technical controls in order to assure proper authorization and security controls verification for applicable CIP assets. The result will improve compliance with the requirements for maintaining accurate baseline documentation. Risk was minimized given that the CIP assets applicable to this self-report had proper controls in place, such as user authorization and authentication, two-factor electronic access controls, and the assets were physically secured within a PSP. Additionally, all of the CIP assets associated with this issue are either EACMS associated with Substation medium impact BES Cyber Systems or PACS assets; these issues did not include any high or medium impact BES Cyber Systems or their associated Protected Cyber Assets. New technical controls implemented will improve compliance with the requirements for CIP-010-2 R1.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitiga ion 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 comp[redacted]s mitigation plan will minimize the [redacted]olations of the same requirements by [redacted]a[redacted] [redacted]cumentat[redacted] help ensure all [redacted] ports are correctly ann[redacted]ed in device baseline d[redacted]tion. [redacted]nally submitted self-repo[redacted] has com[redacted] owing actions t[redacted]t future recurrence: [redacted]
3. Implement a s[redacted] any changes to the Transmission baseline documentation and business justi[redacted]ensure all ports enabled and [redacted]rations are included in t[redacted]associated baseline docu[redacted]tation. Supervisory review shall be captured in the baseline change log. (Completed 10/26/16) [redacted]

Milestone 3 Evidence: [redacted]
CIP-010-2 R1.1 [redacted] This updated version of the [redacted]010-2 Baseline Configuration Change Management Work Practice, in Section 5.1, Step 2, [redacted]at [redacted] implemented a secondary Supervisor review of any changes to t[redacted]smission baseline

[redacted]umentation and bu[redacted]fication[redacted]nd requires that Supervisory [redacted]all be[redacted]seline change log. The work practice was updated on 10/[redacted]6 and approved on [redacted]s noted in the change log on page 12. [redacted]

Ad[redacted]nally, the following provides informa[redacted] to the previously submitted [redacted]

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

Su[redacted]sful completion of this r[redacted]ations of the s[redacted]nting additional technical controls, [redacted]ersonnel, and obtaining additional re[redacted]to provide greater ove[redacted]nt of CIP-010-2 R1 complian[redacted]ansions[redacted]Tech Org h[redacted]eted the [redacted]acti[redacted]e recurrer[redacted]applicable[redacted] IT Work Practice[redacted]1.1 and retrained department personnel on updating baseline documentation within the required timeframes. Completed 12/6/2016 [redacted]rtmental perso[redacted]gn documentatio[redacted]ey have reviewed and understand the applicable procedural steps and agree to abide by the procedures going forward. Completed 12/6/2[redacted]

5)[redacted] Tech Org removed all EACMS[redacted] servers from the [redacted] enterprise management containers, changed them to the All EACMS[redacted], and moved them to a new [redacted]container for future backup agent deploy[redacted]t[redacted]Completed 8/26/2016

7)[redacted] Tech Org exclud[redacted] deplo[redacted]ections) and mo[redacted]them to collections for all future targeted C[redacted]urity Patch deployments. Completed 10/4/2016[redacted]

[redacted]Ops Compliance conducted a review and[redacted]ssion with [redacted]emphasize the importance of compliance with the[redacted] Stand[redacted]Completed 4/25/2017

11)[redacted] Tech Org reviewed[redacted] Work Practices applicable to CIP-010-2 R1 for areas where additional instruction was added to help prevent re-occurrences. Completed by 6/2/2017

12)[redacted] Tech Org implemented organizational changes to the[redacted] structure to provide additional personnel responsible for CIP compliance tasks to prevent future issues of the same or similar requirements. Completed by 6/15/2017

13)[redacted] Tech Org reviewed each configuration management tool to ensure CIP assets were not included into any enterprise rollup groups to prevent unintentional deployment of updates outside the CIP Change Management process where possible. Completed by 6/29/2017

15)[redacted] Tech Org conducted a review / training session with departmental personnel and management on applicable changes to[redacted] IT Work Practices addressing CIP-010-2 R1. Completed by 6/22/2017

16)[redacted] Tech Org Application Support and[redacted] conducted a review / retraining session with PACS system administrators on he process for replacing controller panel hardware. Completed by 6/27/2017

18)[redacted] Tech Org implemented technical controls to perform a line by line comparison between the baseline documentation software inventory and the software actually installed on the systems. Completed 6/9/2017

19)[redacted] Tech Org developed and deployed technical controls to perform a comparison between the baseline configuration ports and services whitelist and the listening ports and services derived from the output of the [redacted] command. Completed 6/9/2017

24)[redacted] Tech Org implemented changes to the [redacted] to limit the number of administrators with the ability to update CIP assets. Completed 7/18/2017

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 SERC and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
  - I am [redacted] of [redacted]
  - I am qualified to sign this Mitigation Plan on behalf of [redacted]
  - I understand [redacted] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendixe 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 SERC and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

SERC Single Point of Contact (SPOC)

VIEW MITIGATION PLAN CLOSURE: CIP-010-2 (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 2/8/2019

This item was marked ready for signature by [redacted] on 2/8/2019

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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.	SERC2016-402496	SERC2016016321
R1.	SERC2016-402520	SERC2016016451

Date of completion of the Mitigation Plan:

[redacted]

Update Baseline Docs

Milestone Completed (Due: 9/6/2016 and Completed 9/6/2016)
Attachments (0)

Update [redacted] Transmission baseline documentation to include the open port.

Review All Other Baseline Docs

Milestone Completed (Due: 10/14/2016 and Completed 10/6/2016)
Attachments (0)

Review [redacted] Transmission baseline documentation to ensure all authorized logical network accessible ports are included.

Supervisor Review Process

Milestone Completed (Due: 10/31/2016 and Completed 10/26/2016)
Attachments (0)

Implement a secondary Supervisor review of any changes to the Transmission baseline documentation and business justifications to ensure all ports enabled and required for operations are included in the associated baseline documentation. Supervisory review shall be captured in the baseline change log.

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

[redacted]on of Mitigating Activities:
1. Update [redacted] Transmission baseline documentation to include the open port. (Completed 9/6/16)
2. Review [redacted] to ensure all authorized logical network accessible ports a[redacted]leted 10/6/16)
3. Implement a secondary Supervisor review of any changes to the Transmission baselin[redacted]entation and business justifications to ensure all ports enabled and required for operations are included in the associated baseline documentation. Supervisory review shall be captured in the baseline change log. (Completed 10/26/16) [redacted]

Details to P[redacted]ecurrence: Execution of the above mitigation steps [redacted] the issue and prevent future recurrence. [redacted]
Additionally, the following provides information related to the previously submitted [redacted] issues.

[redacted] Technology [redacted]
1) [redacted] Tech Org updated [redacted] Host ports and service [redacted]s part of the baseline documentation to include the open [redacted] as it is required for [redacted] Completed 8/25/2016
2) [redacted] Tech Org performed a review of all [redacted] CIP cyber system baseline documentation, and verified all are up to date and accurate, and included any installs, upgrades, or updates implemented prior to July 1, 2016. Completed 11/18/2016
3) [redacted] Tech Org conducted a review session of the applicable [redacted] IT Work Practices addressing CIP-010-2 R1.1 and retrained department personnel on updating baseline documentation within the required timeframes. Completed 12/6/2016
4 [redacted] Tech Org required departmental personnel to sign documentation attesting that they have reviewed and understand the applicable procedural steps and agree to [redacted] the procedures going forward. Completed 12/6/2016

As part of Scope Expansion #1 to issue [redacted], the following milestones start at number 5, which is an extension of the original self-report and the four milestones contained therein. [redacted]
5) [redacted] Tech Org removed all EACM [redacted] se [redacted] from the [redacted] enterprise management containers, changed them to the All EACMS [redacted] servers, and moved them to a [redacted] container for future backup agent deployments. Completed 8/26/2016
6) [redacted] Tech Org updated baseline documentation to reflect the version upgrade to the EMC [redacted] agents for he [redacted] EACMS [redacted] servers. Completed 9/2/2016
7) [redacted] Tech C[redacted]ns from "roll-up" patch deployment collections (including [redacted], [redacted] enterprise deploymen[redacted]ns) and moved them to collections for all future targeted CIP Security Patch dep[redacted] Completed 10/4/2016 [redacted]

8) Tech Org updated the PACS baseline documentation to include the software upgrade. Completed 10/7/2016
9) Tech Org updated the PACS baseline documentation to include the PACS controller panel firmware upgrades and PACS controller replacements. Completed 3/23/2017
10) Ops Compliance conducted a review and oversight session with Executives over the Technology Organization's compliance with the CIP Standards. Completed 4/25/2017
11) Tech Org reviewed IT Work Practices applicable to CIP-010-2 R1 for areas where additional instruction was added to help prevent re-occurrences. Completed by 6/2/2017
12) Tech Org implemented organizational changes to the structure to provide additional personnel responsible for CIP compliance tasks to prevent future issues of the same or similar requirements. Completed by 6/15/2017
13) Tech Org reviewed each configuration management tool to ensure CIP assets were not included into any enterprise rollup groups to prevent unintentional deployment of updates outside the CIP Change Management process where possible. Completed by 6/29/2017
14) Tech Org performed a review of all and PACS baseline documentation, and verified all are up to date and accurate. Completed by 6/29/2017
15) Tech Org conducted a review / training session with departmental personnel and management on applicable changes to IT Work Practices addressing CIP-010-2 R1. Completed by 6/22/2017
16) Tech Org Application Support and the conducted a review / retraining session with PACS system administrators on the process for replacing controller panel hardware. Completed by 6/27/2017
17 Operations Compliance completed a comprehensive review of all required evidence associated with this mitigation plan and prepare and submitted a closure packet for SERC review of these potential violations. Completed by 7/18/2017

As part of Scope Expansion #2 to issue , the following milestones start at number 18, which is an extension of the original self-report and scope expansion #1 and the seventeen milestones contained therein. A consolidated closure package including evidence for all 24 milestones will be provided to SERC upon completion of the last milestone.
18) Tech Org implemented technical controls to perform a line by line comparison between the baseline documentation software inventory and the software actually installed on the systems. Completed 6/9/2017
19 Tech Org developed and deployed technical controls to perform a comparison between the baseline configuration ports and services whitelist and the listening ports and services derived from the output of the command. Completed 6/9/2017
20) Tech Org updated the PACS ports and services whitelist as part of the baseline documentation to include the range) associated with the necessary and service. Completed 6/21/2017
21) Tech Org updated the PACS Workstations SW inventory as part of the baseline documentation to include the upgraded version and the . Completed 6/22/2017
22) Tech Org verified the software was removed from the PACS Workstations. Completed 6/22/2017
23) Tech Org verified the Antivirus software was removed from the PACS Workstations. Completed 6/22/2017
24) Tech Org implemented changes to the to limit the number of administrator's ability to update CIP Assets. Completed 7/18/2017

Description of the information provided to SERC for their evaluation *

Closure Package
Milestone 1
CIP-010-2 The "Change Log" tab of this spreadsheet shows that the Transmission baseline documentation was updated on 9/6/16 to include the originally discovered open that was missing prior.
Milestone 2:
CIP-010-2 R1.1 This spreadsheet documents the review of all of the Transmission baseline documentation, which was completed on 10/6/16. As noted on Row 154, as part of the execution of this milestone review, one additional authorized logical network accessible was discovered to not be included in the previous baseline documentation.
CIP-010-2 R1.1 The "Change Log" tab of this spreadsheet shows that the baseline documentation was updated on 10/5/16 to include the subsequently discovered op or Approval (see Milestone 3).
Milestone 3:
010-2 R1.1 ; This updated version of the Substations CIP-010-2 Baseline Configuration Change Ma ment Work Practic .1, Step 2, shows that implemented a secondary Supervisor review of any chan e Transmission base umentation and business justifications, and requires that Supervisory review shall be captured in the baseline change log. The work practice was updated on 10 6 and approved on 10/26/2016 as n change log on page 12.

Cl e Package Files:
See the file posted on the SFTP Site with the Closure Package Evidence titled:
*S l Notes:
• defines a "CIP Cyber System" as a Cyber Asset or groups of Cyber Assets that are in-scope for the CIP Standards, but that are not BES Cyber Assets; for example – EACMS, PACS, Intermediate Systems, PCAs. Using "CIP Cyber System" is shorthand for avoiding having to write out all of the applicable systems every time.
• Since this mitigation plan has been created, the IT organization has gone through a restructuring and is now called the Technology Organization. You ma e it referred to commonly as o Tech Org mission Owner).

Mi he 1: Completed 8/25/2016
CI 0-2 R1 Page 1 provides the updated "Ports and Services Whit documentation adding , completed 8/25/2016. Pages 2-28, provide vendor documentation requiring . Page 10 provides the specific reference to .

Milestone 2: Completed 11/18/2016
The following documentation provides a review of all CIP Cyber System baseline documentation. The purpose of the reviews was to verify the accuracy of the baseline documentation for the Cyber Assets managed by IT; the reviews were completed on 11/18/2016. The following CIP Cyber Systems were reviewed; . Each is an EACMS associated with Medium Impact BES Cyber Systems at Transmission Substations.
CIP-010-2 R1 provides a whitelist analysis, security patch analysis, and software inventory analysis completed 11/18/2016 of the operating system configuration for the following CIP Cyber Systems; Connector and In addition, an analysis was completed for and the Domain Controller. Pages 1-29 show whitelist analysis, pages 30-35 show security patch analysis, pages 36-48 show software inventory analysis, and pages 49-168 show baseline summary documentation.
The following files contain an analysis of the configuration of the following CIP Cyber Systems: , and Each file contains an analysis document, baseline configuration documentation, ports and services whitelist, security patch documentation, and software documentation.
• CIP-010-2 R1 pages 1-5, baseline documentation review completed 11/18/2016, pages 6-14 supporting documentation.
• CIP-010-2 R1 pages 1-49, baseline documentation review completed 11/18/2016, pages 50-58 supporting documentation.
• CIP-010-2 R1 pages 1-4, baseline documentation review completed 11/18/2016, pages 5-8 baseline documentation.
• CIP-010-2 R1 pages 1-5, baseline documentation review completed 11/18/2016, pages 6-14 baseline documentation.
• CIP-010-2 R1 pages 1-3, baseline documentation review completed 11/18/2016, pages 4-7 baseline documentation.
• CIP-010-2 R1 pages 1-3, baseline documentation review completed 11/18/2016, pages 4-7 baseline documentation.

Milestone 3: Completed 12/6/2016
• CIP-010-2 R1 presentation used to retrain IT employees and managers on the Configuration and Change Management Program. The training sessions were scheduled based on specific departments within IT, the last training session was completed on 12/6/2016.
• CIP-010-2 R1 presentation used to retrain IT employees and managers on the Ports and Services / Whitelist Program. The training sessions were scheduled based on specific departments within IT, the last training session was completed on 12/6/2016.
• CIP-010-2 R1 provides a list of attendees that participated in the CIP Information Protection Program refresher training, and depicts the date, department, and list of attendees for each session.
• CIP-010-2 R1 Configuration Change Management procedure reviewed in

each of the training sessions.
• CIP-010-2 R1 [redacted] Cyber System Management procedure reviewed in each of the training sessions.
• CIP-010-2 R1 [redacted] IT Baseline Creation and Modification Work Procedure reviewed in each of the training sessions.

Milestone 4: Completed 12/6/2016
• [redacted] provides a sample of the attestation completed by each attendee of the retraining sessions attesting that they have reviewed and understand the applicable procedural steps, and agree to abide by the procedures going forward.

Milestone 5: Completed 8/26/2016
• [redacted]; provides a screen capture and explanation for the removal of all EACMS [redacted] servers from the [redacted] enterprise management containers, to the [redacted] management container.

Milestone 6: Completed 9/2/2016
The following files contain the updated baseline documenta ion to reflect the version upgrade for the [redacted] agents for the 4 EACMS [redacted] servers.
• [redacted]; page 2, provides the baseline documentation showing the update was completed on 9/2/2016.
• [redacted] page 2, provides the baseline documentation showing the update was completed on 9/2/2016.
• [redacted].pdf; page 2, provides the baseline documentation showing the update was completed on 9/2/2016.
• [redacted] page 2, provides the baseline documentation showing the update was completed on 9/2/2016.

Milestone 7: Completed 10/4/2016
• [redacted] pages 1-3, provides screen shots demonstrating the exclusion of all CIP PACS systems from [redacted] patch deployment collections.

Milestone 8: Completed 10/7/2016
[redacted], page 2 provides evidence of the update to the PACS baseline documentation to include the [redacted] software upgrade.

Milestone 9: Completed 3/23/2017
• [redacted], pages 3-4 provides evidence of the update to the PACS baseline documentation to include the PACS controller panel firmware upgrades and PACS controller replacements.

Milestone 10: Completed 4/25/2017
• [redacted], provides the list of attendees for the [redacted] Ops Compliance oversight session with Executives over the [redacted] IT organization.
• [redacted] provides the presentation for the [redacted] Ops Compliance oversight session with Executives over the [redacted] IT organization.

Milestone 11: Completed 6/2/2017
The following documentation provides the updated work practices applicable to CIP-010-2 R1 for areas where additional instruction could be added to help prevent re-occurrences.
• [redacted] provides a summary of the before and after modifications to the documentation for each work practice.
• [redacted] provides the modified work practice that applies to the installation of Security Patches applied to IT managed servers and appliances.
• [redacted] provides the modified work practice that applies to OS, firmware, and installed software inventories.
• [redacted] provides the modified work practice that applies to Change Management.
• [redacted] provides the pre-modified work practice that applies to Change Management.
• [redacted] provides the pre-modified work practice that applies to commissioning new cyber assets.

Milestone 12: Completed 6/15/2017
• [redacted]; provides documentation related to organizational changes to the [redacted] IT structure. Page 1 provides an email notification of the posting for a Risk and Compliance Analyst. Pages 2-3, provide the job description for the Risk and Compliance Analyst position. Pages 4-5 demonstrate changes (additions of [redacted] IT leadership) to the [redacted] CIP Governance Framework.

Milestone 13: Completed 6/29/2017
• [redacted] provides evidence of the configuration management tool review to verify CIP assets are not included into any enterprise rollup groups to prevent unintentional deployment of updates outside the CIP Change Management process where possible.
• [redacted] provides a summary of the configuration tool management review.

Milestone 14: Completed 6/29/2017
The following documentation provides a review of all [redacted] and PACS baseline documentation. The purpose of this additional baseline reviews was to reperform the baseline reviews due 11/18/2016 due to discovered errors reported in this SCOPE EXPANSION. The purpose was again to verify the accuracy of the baseline documentation; these new reviews were completed on 6/29/2017. The following CIP Cyber Systems were reviewed: [redacted]. In addition, the PACS panels, workstations, and servers were reviewed.

• [redacted] pages 1-9, baseline documentation review completed 6/20/2017, pages 10-20, supporting documentation.
• [redacted] pages 1-46, baseline documentation review completed 6/27/2017, pages 47-58, supporting documentation.
• [redacted] pages 1-5, baseline documentation review completed 6/21/2017, pages 6-10, supporting documentation.
• [redacted] pages 1-5, baseline documentation review completed 6/14/2017, pages 6-16, supporting documentation.
• [redacted] pages 1-13, Ports and Services Whitelist baseline documentation review completed 6/28/2017, pages 14-17, supporting documentation. Pages 18-31, Security Patch Management baseline documentation review completed 6/27/2017, pages 31-36, supporting documentation. Pages 37-45, Software Inventory baseline documentation review completed 6/18/2017, page 46, supporting documentation.
• [redacted] pages 1-13, Ports and Services baseline documentation review completed 6/2/2017, pages 14-25, supporting documentation. Pages 26-33, Software baseline documentation review completed 6/8/2017, pages 34-49, supporting documentation.
• [redacted] pages 1-22, baseline documentation review completed 6/29/2017, pages 23-34, supporting documentation.
• [redacted] pages 1-3, Ports and Services baseline documentation review completed 6/29/2017, pages 4-8, supporting documentation, pages 9-12, Security Patch Management baseline documentation review completed 6/29/2017, pages 13-31, supporting documentation, pages 32-37, Software baseline documentation review completed 6/9/2017, pages 38-47, supporting documentation.
• [redacted] pages 1-31, baseline documentation review completed 6/29/2017, pages 32-45, supporting documentation.
• [redacted] pages 1-3, baseline documentation review completed 5/1/2017, pages 4-8, supporting documentation.
• [redacted] pages 1-9, baseline documentation review completed 5/24/2017, pages 10-13, supporting documentation.

Milestone 15: Completed 6/22/2017
• [redacted]; provides a sample of the attestation completed by each attendee attesting that they have reviewed and understand the applicable procedural steps, and agree to abide by the procedures going forward.
• [redacted] provides a list of attendees that participated in the [redacted] Work Practices training.
• [redacted] presentation used to retrain employees and managers on applicable changes to [redacted] IT Work Practices addressing CIP-010-2 R1.

Milestone 16: Completed 6/27/2017
• [redacted] provides the meeting notice for the review / retraining session with PACS system administrators on the process for replacing controller panel hardware.
• [redacted] provides the agenda for the review / retraining session with PACS system administrators on the

process for replacing controller panel hardware.
• [redacted] provides the documentation reviewed for the review / retraining session with PACS system administrators on the process for replacing controller panel hardware.
Milestone 17: Closure Package Milestone for [redacted] and Scope Expansion #1. Completed 7/18/2017

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

Milestone 18: Completed 6/9/2017
• [redacted] provides evidence of the implementation of an automated scripting tool which validates the software installed on the PACS devices are approved in the software inventory baseline documentation.

• [redacted]f, provides the Configuration Change Management work practice instructing users to execute the automated scripting tool. Page 14, Section 9, Steps "b. i" and "c. iii", instruct the user to execute the script to validate ports and services. Page 14-15, Section 10, Steps "b. i" and "c. ii", instruct the user to execute the script to validate the software inventory.

Milestone 19: Completed 6/9/2017
• [redacted] provides evidence of the implementation of an automated scripting tool which validates the ports and services available on the PACS devices are approved in the ports and services baseline documentation.

Milestone 20: Completed 6/21/2017
• [redacted], page 2 provides the updated PACS ports and services whitelist baseline documentation to include [redacted] range.

Milestone 21: Completed 6/22/2017
• [redacted], page 2 provides the updated the PACS Workstations SW inventory baseline documentation to include the upgraded [redacted] and the [redacted].

Milestone 22: Completed 6/22/2017
• [redacted], page 1-2 provides the change management record authorizing the removal of the [redacted] from the two PACS Workstations completed 6/22/2017.
o [redacted], pages 3-10, provides the post verification demonstrating the [redacted] software is not installed on the workstation. Pages 11-19, provides the pre verification demonstrating the [redacted] antivirus software is installed on the workstation.
o [redacted] pages 20-27, provides the post verification demonstrating the [redacted]r software is not installed on the workstation. Pages 28-33, provides the pre verification demonstrating the [redacted] antivirus software is installed on the workstation.

Milestone 23: Completed 6/22/2017
• CIP-010-2 R1 [redacted] page 1-2 provides the change management record authorizing the removal of the [redacted] antivirus software form the four PACS Workstations completed 6/22/2017. Pre and Post change documentation is provided for the four workstations which were affected.
o [redacted], pages 3-14, provides the post verification demonstrating the [redacted] antivirus software is not installed on the workstation. Pages 15-26, provides the pre-verification demonstrating the [redacted] antivirus software is installed on the workstation.
o [redacted], pages 27-38, provides the post verification demonstrating the [redacted] antivirus software is not installed on the workstation. Pages 39-50, provides the pre-verification demonstrating the [redacted] antivirus software is installed on the workstation.
o [redacted], pages 51-62, provides the post verification demonstrating the [redacted] antivirus software is not installed on the workstation. Pages 63-74, provides the pre-verification demonstrating the [redacted] antivirus software is installed on the workstation.
o [redacted], pages 75-86, provides the post verification demonstrating the [redacted] antivirus software is not installed on the workstation. Pages 87-98, provides the pre-verification demonstrating the [redacted] antivirus software is installed on the workstation.

Milestone 24: Completed 7/18/2017
• [redacted] provides documentation of changes to the [redacted] to limit the number of administrators with the approved access to update CIP Assets.

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.

VIEW SELF-REPORT: CIP-010-2 R1. (COMPLETED)

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

This item was submitted by [redacted] on 2/2/2018

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:	[redacted]
NERC Registry ID:	[redacted]
JRO ID:	[redacted]
CFR ID:	[redacted]
Entity Contact Information:	[redacted]

REPORTING INFORMATION

Applicable Standard:	[redacted]
Applicable Requirement:	[redacted]
Applicable Sub Requirement(s):	[redacted].
Applicable Functions:	[redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered:	No
Has this Possible Violation previously been reported to other Regions:	No
Date Possible Violation was discovered:	10/9/2017
Beginning Date of Possible Violation:	11/18/2016
End or Expected End Date of Possible Violation:	10/12/2017
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

On 1[redacted]yee discovered a potential CIP-010-2 R1.4 issue while performing device maintenance at a medium impact subst[redacted] ([redacted]). It was determined the local password for the front panel administrator account on [redacted] Radios (medium impact BES Cyber Systems) was set to the factory default password. Upon discovery, the administrator account password for the front panel was changed on the [redacted] devices from the default password to a unique complex password on 10/12/2017. A review of all past changes completed to the [redacted] devices [redacted]t caused the resetting of the default account password. However, post-change controls checks as per R1.4 failed to confirm device passwords had not been reset. Therefore, the potential scope of non-compliance for the [redacted] devices was 328 days, (11/18/2016 – 10/12/2017).

As a result of this issue, [redacted] completed a review of account passwords between 10/9/2017 and 11/8/2017 of all [redacted] Radios currently on the CIP asset inventory at [redacted] medium impact substations that had received firmware upgrades. On 10/11/2017, it was discovered the local password for the front panel administrator account on [redacted] Radios (medium impact BES Cyber Systems) at a [redacted] medium impact substation [redacted]) was also reset to the factory default password. Upon discovery, the administrator account password for the front panel was changed on the [redacted] devices from the default password to a unique complex password on 10/12/2017. A review of all past changes completed on the [redacted] devices found an authorized firmware update was completed on 12/16/2016 that caused the resetting of the default account password. However, post-change controls checks as per R1.4 failed to confirm device passwords had not been reset. Therefore, the potential scope of non-compliance for the [redacted] devices was 300 days, (12/16/2016 – 10/12/2017).

As part of the extent of condition review, [redacted] also contacted other [redacted] notify them of the potential issue.
- [redacted]) has [redacted] Radios across [redacted] medium impact substations. [redacted] confirmed the local panel password on the [redacted] radios was set to a unique complex password following firmware upgrades.
- [redacted]) has [redacted] Radios located in 1 medium impact substation. [redacted] confirmed the local panel password on the [redacted] radios was set to a unique complex password. [redacted]
- [redacted]) does not have [redacted] radios in their medium impact substations.

The root cause of this issue was a failure to follow the [redacted], [redacted], which requires pre- and post-change control checks be performed and documented at the time of the firmware upgrade. In addition, a failure to follow the [redacted]-Transmission Substations CIP-010-2 Baseline Configurati[redacted]nge Management Work Practice, Section 3.4 Transmission Employee, Step 2, requires assessing the security controls on the device that may be impacted prior to the change, and verifying after completing the baseline configuration change that those security controls were not adversely impacted.

Authorization for the software installation was completed at the time of the change in accordance with CIP-010-2 R1.2. However, the pre- and post-change cyber security controls verification performed at the time of the change as per CIP-010-2 R1.4 failed to include verification that the company-specific applied complex passwords had not been reset to default values.

In order to mitigate this issue and prevent reoccurrence, [redacted] will add additional instruction to the CIP-010-2 Baseline Configuration Change Management Work

Practice as an additional guide for testing CIP-005 and CIP-007 security controls. In addition, [redacted] will perform training on the [redacted] [redacted] [redacted], [redacted] and the Updated CIP-010-2 Baseline Configuration Change Management Work Practice with the appropriate personnel to ensure thorough understanding of the security controls within standards CIP-005 and CIP-007 to be verified following baseline changes.

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

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

1) [redacted] will change the local default administration account password on the [redacted] substation [redacted] Radios.
2) [redacted] will change the local default administration account password on the [redacted] substation [redacted] Radios.
3) [redacted] will conduct a review / training session with [redacted] [redacted] and [redacted] personnel on the CIP-010-2 Baseline Configuration Change Management Work Practice.
4) [redacted] will add additional instruction to the CIP-010-2 Baseline Configuration Change Management Work Practice as an additional guide for testing CIP-005 and CIP-007 security controls.
5) [redacted] will conduct an additional review / training session with [redacted] Services and [redacted] personnel on the CIP-010-2 Baseline Configuration Change Management Work Practice.
6) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

4/30/2018

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Update [redacted] Trans Subs Work Practice	3/1/2018	4) [redacted] will add additional instruction to the CIP-010-2 Baseline Configuration Change Management Work Practice as an additional guide for testing CIP-005 and CIP-007 security controls.	Yes
Reinforce [redacted] Trans Sub WP and Train on Changes from MS 4	4/10/2018	5) [redacted] will conduct an additional review / training session with [redacted] and [redacted] personnel on the CIP-010-2 Baseline Configuration Change Management Work Practice.	Yes
Closure Package	4/30/2018	6 [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review.	No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue posed a minimal potential risk, and not a serious or substantial risk to the reliability of the bulk electric system [redacted] Potential risk could include the introduction of unknown vuln [redacted] and configuration changes susceptible to exploitation by not following documented processes and verifying security controls are in place after performing the firm [redacted] e was a failure to follow the [redacted] CIP Policy and Procedures Manual, [redacted], which requires pre- and post-change control checks be performed and documented. In addition, a failure to follow the [redacted] [redacted]

The [redacted] are not configured for interactive remote access, however, this oversight could have potentially allowed access to the device by someone knowledgeable of the vendor default account passwords, but those personnel would have to be physically standing at the device, which is protected within a PSP.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk, and not a serious or substantial risk to the reliability of the bulk electric system. [redacted] failure to change the administrator account password on the [redacted] radio could have allowed a user with authorization for physical access to the Substation PSP the ability to modify the configuration of the device. However, the CIP [redacted] monitors for unauthorized a [redacted] tion 24/7. [redacted] [redacted] [redacted]

In al [redacted] e remote access is not configured for these devices, they are physically protected within a PSP, and other logical protections for other devices within the PSP are in place to further minimize the actual possibility of the introduction of unknown vulnerabilities and configuration changes.

Additional Comments:

The [redacted] that specifically address requirements and processes around complying with CIP-010-2 R1.4. Additionally, [redacted] T [redacted] on Substations has the CIP-010-2 Baseline Configuration Change Management Work [redacted] addressing compliance with CIP-010-2 R1.4. [redacted] [redacted]

[redacted]:
Section 4.2 Determination and Testing of Required Cyber Security Controls, CIP-010-2 R1.4 [redacted]
The list of required cyber security controls in CIP-005 and CIP-007 for High- and Medium-Impact BES Cyber Systems and their associated EACMS, PACS and PCAs are listed in Attachment 1 – Cyber Security Controls. The elements of a baseline configuration required to be captured include operating system/firmware, commercial

software, custom softwa[redacted]ogical network accessible ports, and security patches. [redacted]

Appropriate[redacted]Unit Personnel shall determine which of the required[redacted]ity controls in Attachment 1[redacted]er Security Controls may be impacted by a requested change to the baseline configuration of a High- or Medium-Impact BES Cyber System and its associated EACMS, PACS, and PCA prior to authorizing the change, and shall document the verification or results of testing that[redacted]uired cyber security controls were not adversely affected after the change is completed.

CIP-010-2 Baseline Configuration Change[redacted]ent Work Practice
Section 3.4 Transmission Employee
An employee with the authorization and [redacted]rience to make chang[redacted] NERC CIP substations is responsible for the following:
1.[redacted]rk Or[redacted]r CIP Authorizer [redacted]he Work Order Creator is unav[redacted]le), prior to implementing the baseline config[redacted]hange.
2. Assessing the security controls (see Section 5.2) in the device that may be impacted prior to the change, and verifying after completing the baseline configuration ch[redacted]e not [redacted]mpacted. [redacted]
3. Ensuring that all required evidence is obtained and submitted to the appropriate [redacted] Relay Work Order Creator for the workgroup.
4.[redacted] when the work h[redacted]completed and the work order can be closed.

Section 5.2 Completing the Baseline Configuration Ch[redacted]
It is extremely important to populate he CIP Baseline Configuration [redacted]nge Record ID field with the work order (WO) number from [redacted]. This is needed to link the form with the work order for evidence purposes. Contact your department's CIP Authorizer or [redacted] if assistance is needed with completing the fields.

The [redacted] radio is a transmitter and/or receiver that is utilized to provide tripping or blocking information to relays at each end of a single transmission line. The radio allows the line relays to communicate by sending and receiving a signal of a specified frequency. The frequency and bandwidth can be changed on these devices from the front panel.

[redacted]

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW MITIGATION PLAN CLOSURE: CIP-010-2 (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 4/27/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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.	SERC2018-402974	SERC2018019106

Date of completion of the Mitigation Plan:

[redacted]

Update [redacted] Trans Subs Work Practice

Milestone Completed (Due: 3/1/2018 and Completed 2/28/2018)
Attachments (0)

4) [redacted] he CIP-010-2 Baseline Configuration Change Managem [redacted] 05 and [redacted]

Reinforce [redacted] Trans Sub WP and Train on Changes from MS 4

Milestone Completed (Due: 4/10/2018 and Completed 4/10/2018)
Attachments (0)

5) [redacted] will conduct an additional review / training session with [redacted] and [redacted] personnel on the CIP-010-2 Baseline Configuration Change Management Work Practice.

Closure Package

Milestone Completed (Due: 4/30/2018 and Completed 4/27/2018)
Attachments (0)

6) [redacted] Op [redacted] a comprehensive review of all required evidence asso [redacted] osure [redacted]

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

Description of Mitigating Activities:
1) [redacted] will change the local default administration account password on the [redacted] substation [redacted] Radios. Completed 10/12/2017

2) [redacted] will change the local default administration account password on the [redacted] substation [redacted] Radios. Completed 10/12/2017

3) [redacted] will conduct a review / training session with [redacted] and [redacted] personnel on the CIP-010-2 Baseline Configuration Change Management Work Practice. Completed 1/10/2018

4) [redacted] SIA will add additional instruction to the CIP-010-2 Baseline Configuration Change Management Work Practice as an additional guide for testing CIP-005 and CIP-007 security controls. Completed 2/28/2018

5) [redacted] will conduct an additional review / training session with [redacted] and [redacted] personnel on the CIP-010-2 Baseline Configuration Change Management Work Practice. Completed 4/10/2018

6) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Completed 4/27/2018

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

Milestone 1: Completed 10/12/2017
[redacted], provides email evidence the local default administration account password on the [redacted] substation [redacted] Radios was changed.

Milestone 2: Completed 10/12/2017
[redacted], provides evidence the local default administration account password on the [redacted]

Radios was changed.

Milestone 3: Completed 1/10/2018

[redacted] provides the meeting agenda and attendee list for the review / retraining [redacted] personnel on the CIP-010-2 Baseline Configuration Change Management Work Practice.

[redacted] presentation used to retrain [redacted] employees and managers on the CIP-010-2 Baseline Configuration Change Management Work Practice.

Milestone 4: Completed 2/28/2018

[redacted], provides the modified Transmission Substations work practice for CIP-010-2 Baseline Configuration Change Management where [redacted] added the following additional guidance: Page 5, clarification that baseline changes are not to be made prior to work order approval; Page 6, highlighted aspects of the security control verification process; Page 7, clarification for failed IED replacement processes; and Pages 11-13, Appendices 8.2-8.4 to add more templates for field employee use for security control verifications for testing CIP-005 and CIP-007 security controls.

Milestone 5: Completed 4/10/2018

[redacted], provides the meeting agenda and attendee list for the review / retraining of [redacted] personnel on the CIP-010-2 Baseline Configuration Change Management Work Practice. Training sessions were scheduled based on specific departments within [redacted], and two makeup training sessions were completed. The last training session was completed on 4/10/2018.

[redacted], is the presentation used to retrain [redacted] and affiliate operating company [redacted] employees and managers on updates to the CIP-010-2 Baseline Configuration Change Management Work Practice.

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.

Attachment 14

Record documents for the violation of CIP-011-2 R1

14a. The Entities' Self-Report (SERC2016016379)

14b. The Entities' Certification of Mitigation Plan Completion submitted December 8, 2016

14c. The Entities' Self-Report (SERC2016016572)

14d. The Entities' Certification of Mitigation Plan Completion submitted March 1, 2019

14e. The Entities' Self-Report (SERC2017017564)

14f. The Entities' Mitigation Plan designated as SERCMIT014401 submitted September 4, 2018

14g. The Entities' Certification of Mitigation Plan Completion submitted September 4, 2018

VIEW SELF-REPORT: CIP-011-2 R1. (COMPLETED)

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

This item was submitted by [redacted] on 11/28/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:	[redacted]
NERC Registry ID:	[redacted]
JRO ID:	[redacted]
CFR ID:	[redacted]
Entity Contact Information:	[redacted]

REPORTING INFORMATION

Applicable Standard:	[redacted]
Applicable Requirement:	[redacted]
Applicable Sub Requirement(s):	[redacted]
Applicable Functions:	[redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered:	No
Has this Possible Violation previously been reported to other Regions:	No
Date Possible Violation was discovered:	9/14/2016
Beginning Date of Possible Violation:	7/1/2016
End or Expected End Date of Possible Violation:	9/15/2016
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

On September 14, 2016, [redacted] disclosed to [redacted] Transmission Compliance that drawings containing BES Cyber System Information were inadvertently stored in a manner that did not comply with [redacted] documented NERC CIP Information Protection Procedure [redacted] Prior to July 1, 2016, physical copies of documents containing BES Cyber System Information were modified in order to remove BES Cyber System Information (BCSI) from an electronic copy of the same documents. Upon modification, the original physical documents containing BCSI were to be destroyed. On September 14, 2016, it was discovered that some of the original physical documents containing BCSI were not destroyed. Upon discovery of these physical documents, a review of the relevant work areas, including all [redacted] business offices and all Medium-Impact BES Cyber System locations where storage of these drawings was known was conducted to determine the full scope of the issue. All hard copy documents containing BES Cyber System Information were destroyed on September 15, 2016. The scope of non-compliance is from July 1 through September 15, 2016 (77 Days).

[redacted] documented NERC CIP Information Protection Procedure [redacted] in [redacted] Information Handling, requires that BES Cyber System Information shall be stored in a controlled access environment to ensure it is protected, and requires that the functional department head shall maintain a list of all controlled access repositories containing BES Cyber System Information along with the access approver(s) for each repository. The documents at issue were not stored in a documented controlled access repository.

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

1. [redacted] office areas to locate all hardcopy files with BES Cyber System Information to confirm all printed files are stored correctly or have been shredded. (Completed 9/15/2016)
2. Destroy all documents with BES Cyber System Information that were stored incorrectly. (Completed 9/15/2016)
3. Retrain [redacted] employees on [redacted] NERC CIP Information Protection Procedure [redacted]. (Completed 11/8/2016)

Provide details to prevent recurrence:

Su[redacted] of the above mitigation plan milestones will prevent future recurrence of this issue.

[redacted] [redacted]

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

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

11/8/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue poses a minimal potential risk, and not a serious or substantial potential risk to the bulk power system. The drawings were specific [redacted] Substation drawings [redacted] which included device mode[redacted]unication path information between devices within the same ESP. Unauthorized disclosure could have aided in the potential of unauthorized access.

Provide detailed description of Actual Risk to Bulk Power System:

This issue poses a minimal actual risk, and not a serious or substantial actual risk to the bulk power system. The diagrams in question were p[redacted]ted within company l[redacted]ed using badge readers and [redacted] authorization for access. However, the storage locations were not on the designated list of BES Cyber System Information repositories as required by [redacted]. During the review, there was no indication of physical access to the drawings by unauthorized personnel. In addition, the diagrams alone would be insufficient in providing unauthorized access and would require additional information.

Additional Comments:

[redacted] [redacted] [redacted]

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW MITIGATION PLAN CLOSURE: CIP-011-2 (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 12/8/2016

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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.	SERC2016-402511	SERC2016016379

Date of completion of the Mitigation Plan:

[redacted]

[redacted] file moved to BCSI Repository

Milestone Completed (Due: 7/29/2016 and Completed 7/29/2016)
Attachments (0)

[redacted] file will be moved to a [redacted] epository. [redacted]

Password Change

Milestone Completed (Due: 7/29/2016 and Completed 7/29/2016)
Attachments (0)

[redacted] d to access the (CIP) [redacted] file will be changed and provided verba [redacted] those resources with authorized access.

Confirm BCSI storage

Milestone Completed (Due: 11/30/2016 and Completed 11/30/2016)
Attachments (0)

[redacted] erform a review to veri [redacted] are no additional instances of BCSI that [redacted] IT owns or manages that is not properly stored in a documented BCSI repository.

Retraining

Milestone Completed (Due: 11/30/2016 and Completed 11/15/2016)
Attachments (0)

[redacted] train department pers [redacted] d managers on the [redacted] CIP Informat [redacted] Protection Program to ensure prevention of future recurrence of this issue.

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

Description of Mitigating Activities:
1) The [redacted] file will be moved to a BCSI Repository.
2) The password to access the (CIP) [redacted] file will be changed and provided verbally to those resources with authorized access.
3) [redacted] IT will perform a review to verify there are no additional instances of BCSI that [redacted] IT owns or manages that is not properly stored in a documented BCSI repository.
4) [redacted] IT will retrain department personnel and managers on the [redacted] CIP Information Protection Program to ensure prevention of future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

Milestone 1:
[redacted] Page 1 - Provides a confirmation attestation that the [redacted] file was moved to a documented BCSI repository as of 7/29/2016, and Page 2 - provides a screenshot of the BCSI repository the [redacted] is stored in, effective 7/29/2016 ([redacted]

Milestone 2:
[redacted] Page 1 thru 3 - Provides documentation via an [redacted] IT procedure evidence template that the shared password for the [redacted] Hosts contained in the protected [redacted] file were changed as of 7/29/2016; Page 4 – provides a list of the individuals with authorization in the AMA entity " [redacted] " approved to access the new BCSI repository folder location where the [redacted] file is now located, and approved to verbally receive the new [redacted] file password; Page 5 – provides a log maintained by the department manager documenting when the [redacted] file password used for accessing the contents of the [redacted] file was changed (on 7/29/2016) , and to which resources the new password was issued.

Milestone 3:
[redacted] this spreadsheet contains the results of the review performed by [redacted] IT using the [redacted] tool to verify there were no additional instances of BCSI that [redacted] IT owns or manages that was not properly stored in a documented BCSI

repository. Column "H" represents the categorization of the data determined during the review, and column "U" provides the completion date of the review for each line item.

[redacted] this document provides a summary attestation of the analysis completed on the [redacted] scan results for BCSI information on 11/30/2016. No additional instances of BCSI were found outside of an [redacted] IT approved BCSI repository.

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

Milestone 4:

[redacted] Presentation used to retrain [redacted] IT employees and managers on the [redacted] CIP Information Protection Program. The training sessions were scheduled based on specific departments within IT, and the last training session was completed on 11/15/2016.

[redacted] Provides a list of attendees that participated in the [redacted] CIP Information Protection Program refresher training, and depicts the date, department, and list of attendees for each session.

[redacted] Information Protection Program reviewed in each of the training sessions.

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.

VIEW SELF-REPORT: CIP-011-2 R1. (COMPLETED)

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

This item was submitted by [redacted] on 10/19/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:	[redacted]
NERC Registry ID:	[redacted]
JRO ID:	[redacted]
CFR ID:	[redacted]
Entity Contact Information:	[redacted]

REPORTING INFORMATION

Applicable Standard:	[redacted]
Applicable Requirement:	[redacted]
Applicable Sub Requirement(s):	[redacted]
Applicable Functions:	[redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered:	No
Has this Possible Violation previously been reported to other Regions:	No
Date Possible Violation was discovered:	7/20/2016
Beginning Date of Possible Violation:	7/1/2016
End or Expected End Date of Possible Violation:	7/29/2016
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

On July 20th, 2016, an [redacted] IT Manager discovered a file containing shared user account passwords for the [redacted] Host servers stored in an undocumented BCSI repository. As of July 1, 2016, the [redacted] Host servers were categorized as EACMS associated with Medium Impact BES Cyber Systems. The manager had intended to move the file from it's current location to an existing BCSI repository on or before July 1, 2016, but failed to do so until July 29, 2016.

Prior to the CIP V5 implementation on July 1, 2016, the [redacted] Team stored their shared account passwords in an encrypted and password protected [redacted] file located in a protected folder on the corporate network shared drive. Access to the protected folder was controlled by having membership granted in the [redacted] based on departmental business need, and the password used to access the contents of the [redacted] file was provided verbally by the manager to those [redacted] Admins who were authorized and required access. When an employee became a member of the [redacted] Team they were added to the [redacted] to access the folder location of he file, and were provided the file password by the manager.

Upon discovery of the encrypted and password protected file containing the shared user account passwords for the [redacted] Host servers being stored in an undocumented BCSI repository on July 20th, 2016, the [redacted] file was moved to a documented BCSI repository on July 29, 2016. Access to the BCSI repository is controlled by requesting and being approved for access in [redacted]. In addition to the change in the storage location, the [redacted] file master key password was changed and reissued to authorized personnel on July 29, 2016.

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

1) The [redacted] file will be moved to a BCSI Repository. Completed 7/29/2016
2) The password to access the (CIP) [redacted] file will be changed and provided verbally to those resources with authorized access. Completed 7/29/2016
3) [redacted] IT will perform a review to verify there are no additional instances of BCSI that [redacted] IT owns or manages that is not properly stored in a documented BCSI repository. (11/30/2015)
4) [redacted] IT will retrain department personnel and managers on the [redacted] CIP Information Protection Program to ensure prevention of future recurrence of this issue. (11/30/2016)

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

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

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

11/30/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
[redacted] file moved to BCSI Repository	7/29/2016	The [redacted] file will be moved to a BCSI Repository.	No
Password Change	7/29/2016	The password to access the (CIP) [redacted] file will be changed and provided verbally to those resources with authorized access.	No
Confirm BCSI storage	11/30/2016	[redacted] IT will perform a review to verify there are no additional instances of BCSI that [redacted] IT owns or manages that is not properly stored in a documented BCSI repository.	No
Retraining	11/30/2016	[redacted] IT will retrain department personnel and managers on the CIP Information Protection Program to ensure prevention of future recurrence of this issue.	Yes

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue posed a minimal potential risk and did not pose a serious or substantial potential risk to the reliability of the bulk power system. The root cause of this issue was a failure to properly store BCS Information in a documented BCSI Repository. The potential for a possible unauthorized access or disclosure of the BCSI contained within the [redacted] file was not probable based on the below mitigating factors.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk and did not pose a serious or substantial actual risk to the reliability of the bulk power system. The root cause of this issue was a failure to properly store BCS Information in a documented BCSI Repository. In order to access the [redacted] file, a resource had to have access to both the storage location of the file and the file's master password. Access to the folder location of the file was managed by membership in an Access Control List maintained by the department manager, and contained only those personnel with a business need for access in that department. In addition, the department manager also maintained the file's master password, and only issued the password verbally to those with a business need for access in her department. The resources which had access to both the folder location of the file, and the file's master password prior to this issue are the same as those reissued the new password on 7/29/2016.

Additional Comments:

[redacted]

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW MITIGATION PLAN CLOSURE: CIP-011-2 (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 3/1/2019

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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.	SERC2016-402548	SERC2016016572

Date of completion of the Mitigation Plan:

[redacted]

No Milestones Defined

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

Description of Mitigating Activities:

1. Review [redacted] office areas to locate all hardcopy files with BES Cyber System Information to confirm all printed files are stored correctly or have been shredded. (Completed 9/15/2016)
2. Destroy all documents with BES Cyber System Information that were stored incorrectly. (Completed 9/15/2016)
3. Retrain [redacted] employees on [redacted] NERC CIP Information Protec ion Procedure [redacted]. (Completed 11/8/2016)

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

As part of the mitigating items for the subsequently filed scope expansion [redacted]:

1. [redacted] will require managers to review all individuals with View Passwords role in [redacted] to determine if the scope of individuals with this role can be reduced to further restrict access to passwords where needed. Due by 3/31/2017, Completed 3/31/2017
2. [redacted] will draft a [redacted] specifically addressing the proper protection and secure handling of BES Cyber System Information, including storage, transit, and use, where applicable, and new request processes and secure storage of passwords. Due by 4/28/2017, Completed 4/18/2017.
3. [redacted] and [redacted] Transmission Compliance will conduct retraining of all personnel with View Passwords role in [redacted] on the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and train personnel on Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use. Due by 4/28/2017, Completed 4/25/2017.
4. [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Due by 5/12/2017, Completed 5/12/2017

Description of the information provided to SERC for their evaluation *

For the original [redacted] Self-Report and Mitigation Plan Milestones, the following evidence has been provided:

Milestone 1 & Milestone 2:
[redacted] This document depicts email confirmation that [redacted] reviewed all hardcopy drawing files for NERC CIP Facilities maintained by [redacted] for unprotected BES Cyber System Information and remediated, where necessary, any of these drawings by 9/15/2016.
[redacted] This document shows the office areas reviewed, and reflects that all the relevant hardcopy files were located and confirmed to be correctly stored or destroyed as of 9/15/16.

Milestone 3:
[redacted] This outlook meeting invitation shows the time, date (10/26/16), and attendees present at [redacted] training, which included training regarding [redacted] NERC CIP Information Protection Procedure [redacted].
[redacted] This meeting agenda shows, on pages 1 and 2, that [redacted] NERC CIP Information Protection Procedures were covered in the 10/26/16 training session.
[redacted] This outlook meeting invitation shows the time, date (11/8/16), and attendees present at [redacted] Information Protection training.
[redacted] This meeting agenda shows that [redacted] NERC CIP Information Protection Procedures were covered in the 11/8/16 training session.

For the scope expansion [redacted] and Mitigation Plan Milestones, the following evidence has been provided:

Milestone 1
[redacted]; This document depicts email confirmation that [redacted] and [redacted] reviewed all individuals with access to shared passwords in [redacted] to determine if the scope of individuals with this role can be reduced to further restrict access to passwords, where needed, by 3/31/2017; where the scope of personnel could be reduced, a screenshot has been included from the [redacted] Access Management Application ([redacted]) showing a revocation of authorization for the roles of View Passwords.

Milestone 2:

[redacted]; This document depicts the [redacted] developed specifically to reinforce the proper protection and secure handling of BES Cyber System Information, including storage, transit, and use, where applicable, and new [redacted] processes to ensure the secure storage of passwords. The [redacted] was approved by Substations Management on 4/18/2017.

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

Milestone 3:

[redacted] This document shows the time, date, and attendees present at various [redacted] training sessions, as well as an [redacted] training session, which included training regarding the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use.

[redacted] This document shows the distribution on 4/25/2017 of re-training materials regarding the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use to [redacted] personnel, as well as [redacted] personnel with access to [redacted] shared passwords.

[redacted] This document shows the attendees present at [redacted] training session on 4/25/17, which included training regarding the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use.

[redacted] This document shows the distribution on 4/6/2017 and attestation of completion on 4/22/2017 of re-training materials regarding the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use to the one [redacted] employee with access to [redacted] shared passwords.

[redacted] This powerpoint presentation shows the content of retraining materials used by each operating company group conducting reinforcement training with individuals with access in [redacted] to shared passwords. This training covered the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use.

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.

VIEW SELF-REPORT: CIP-011-2 R1. (COMPLETED)

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

This item was submitted by [redacted] on 5/15/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in this link to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [redacted]

NERC Registry ID: [redacted]

JRO ID: [redacted]

CFR ID: [redacted]

Entity Contact Information: [redacted]

REPORTING INFORMATION

Applicable Standard: [redacted]

Applicable Requirement: [redacted]

Applicable Sub Requirement(s): [redacted].

Applicable Functions: [redacted]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

SERC2016016572

Date Reported to Region or Discovered by Region:

11/28/2016

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

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

Date Possible Violation was discovered: 2/3/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 5/12/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On March 14, 2017, [redacted] an [redacted], self-reported a potential violation of CIP-011-2 R1.2 as a scope expansion to a previous [redacted] CIP-011-2 R1.2 self-report (SERC2016-402548) when it was discovered [redacted] personnel had inadvertently stored and transmitted via e-mail unencrypted shared account passwords for Medium Impact BES Cyber Systems in a manner that did not comply with [redacted] documented NERC CIP Information Protection Procedure [redacted] To determine the extent of condition of that issue, [redacted] Operations Compliance conducted an internal investigation with employees at each affiliated Operating Company with the ability to view or access device passwords in the Substations database ([redacted]) to determine if any additional instances of improper storage or unauthorized transmission of shared passwords has occurred. As a result of this internal investigation, additional instances of improper storage and e-mail transmission of shared account passwords were discovered within [redacted].

As of February 3, 2017, [redacted] Transmission Compliance identified [redacted] employees (out of [redacted] personnel with access to passwords) that were found to have improperly stored and/or emailed relay spreadsheets downloaded from the Substations database ([redacted]) containing unencrypted device shared account passwords for [redacted] Substation Medium Impact BES Cyber Systems. The [redacted] personnel stored the relay documents on corporate network drive locations and local drives on company issued laptops that were not identified and authorized as BES Cyber System Information (BCSI) repositories. The relay documents were also exchanged via e-mail between [redacted], [redacted] Applications, and Transmission Maintenance Center personnel as a part of performing relay maintenance activities. These [redacted] employees had authorization to view and obtain Medium Impact BES Cyber System (relay) shared account passwords in the [redacted] BCSI repository. However, the improper storage and transmission via e-mail of this BCSI by these [redacted] out of [redacted] total personnel in [redacted] did not comply with [redacted] documented NERC CIP Information Protection Procedure [redacted].

To prevent future recurrence of inadvertent downloading of shared account passwords, [redacted] updated configuration settings within the [redacted] application where these shared account passwords are stored to remove shared passwords from any default export of Substation device information. Asset owners of the Substations database

[redacted] and managers of personnel with the ability to view passwords in the database conducted a review to determine if the number of personnel with access to passwords could be reduced to limit scope and to take steps to reduce the likelihood of recurrence.

As part of the extent of condition review by [redacted] Operations Compliance, an internal investigation was conducted with [redacted] with the ability to view or access device passwords in [redacted] to determine any additional instances of improper storage or unauthorized transmission of shared passwords has occurred. No additional instances of improper storage or transmission of BCSI were found to have occurred at [redacted] as they have a much smaller number of assets and personnel with the ability to access the Substations database ([redacted]). All [redacted] personnel and [redacted] personnel with the ability to view or access device passwords in [redacted] confirmed that there were no additional instances of improper storage or transmission of this BCSI.

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

1) [redacted] will require managers to review all individuals with View Passwords role in [redacted] to determine if the scope of individuals with this role can be reduced to further restrict access to passwords where needed. Completed 3/31/17.
2) [redacted] will draft a [redacted] specifically addressing the proper protection and secure handling of BES Cyber System Information, including storage, transit, and use, where applicable, and new request processes and secure storage of passwords. Completed 4/28/2017
3) [redacted] and [redacted] Transmission Compliance will conduct retraining of all personnel with [redacted] role in [redacted] on the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and train personnel on Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use. Completed 4/28/2017
4) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Completed 5/19/2017

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Date Mitigating Activi ies (including activities to prevent recurrence) are expected to be completed or were completed:

5/19/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Closure Package to SERC	5/19/2017	[redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.	No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This issue poses a minimal potential risk, and not a substantial potential risk to the bulk power system. Unauthorized storage and disclosure of the shared account passwords in question could have aided in the potential of unauthorized electronic access if personnel also had authorized physical access to the PSPs where these devices are located. Personnel would have had to obtain shared relay passwords in combination with physical access, relay terminal software, and relay usage knowledge to be capable of changing device settings, flash firmware, or close contacts leading to a trip of a breaker on the bulk power system. Alternatively, knowledge of the device passwords, in combination with authorization for Interactive Remote Access, could allow a user the ability to change device passwords and potentially temporarily lock others out of the system. Unauthorized changes of device passwords in combination with other potential device setting changes could affect the way a device was designed to operate.

Provide detailed description of Actual Risk to Bulk Power System:

This issue poses a minimal actual risk, and not a serious or substantial actual risk to the bulk power system. The spreadsheets in question were stored on a business unit shared drive, but the location these spreadsheets were temporarily stored in was not on the designated list of BES Cyber System Information repositories as required by [redacted]

The individuals that received via e-mail the shared account passwords in question did have current authorization to view or access those passwords, and all of these employees do have active authorization for other electronic and/or physical access to CIP areas or systems, which requires a valid, compliant background check and the completion of annual NERC CIP training. In addition, knowledge of these passwords alone would not provide the ability for unauthorized electronic, interactive remote, or physical access to these devices. Upon discovery, the passwords in question were deleted from the shared drive locations, and a review of the individual's e-mail files/folders confirmed all instances of the e-mails in question had been deleted.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4)

VIEW FORMAL MITIGATION PLAN: CIP-011-2 (REGION REVIEWING MITIGATION PLAN)

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

This item was signed by [redacted]) on 9/4/2018

This item was marked ready for signature by [redacted] on 8/31/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-011-2 R1.	SERC2017017564	SERC2017-402689	05/15/2017	Revision Requested	Informal	
CIP-011-2 R1.	SERC2017017564	SERC2017-402689	09/04/2018	Region reviewing Mitigation Plan	Formal	1

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

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

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

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name: [redacted]

Company Address: [redacted]

[redacted]

Compliance Registry ID: [redacted]

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

Name: [redacted]

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

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

Standard: [redacted]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R1.	SERC2017-402689	SERC2017017564	5/15/2017

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

On Ma[redacted]h 14, 2017, [redacted] ported a potential violation of CIP-011-2 R1.2 as a scope expansion to a previous [redacted] CIP-01[redacted]1.2 self-report (SERC2016-4[redacted] tted via [redacted]r Medium Impact BES Cyber Systems in a manner that did not comply with [redacted] documented NERC CIP Information Protection Procedure [redacted]. To determine the extent of condition of that issue, [redacted] Operations Compliance conducted an internal investigation with employees at each affiliated Operating Company with the ability to view or access de[redacted]swords in the Substations database [redacted] to determine if any additional instances of improper storage or unauthorized transmission of shared passwords had occurred. As a result of this internal investigation, additional instances of improper storage and e-mail transmis[redacted]d account pas[redacted]hir[redacted]. No issues related to CIP-011-2 R1 were discovered at [redacted] or [redacted] due to a much smaller scope of personnel with access to this information, and a much smaller scope of assets being managed under this program. The issues dis[redacted]n [redacted] were found[redacted] result of the extent of condition revie[redacted]erformed for [redacted]

As of February 3, 2017, [redacted] Transmission Compliance identified [redacted] employees (out of [redacted] personnel with access to passwords) that were found to have improperly stored and/or emailed relay spreadsheets downloaded f[redacted]t[redacted]Substations database ([redacted]) containing [redacted]rypted device shared account passwords for [redacted] Substation Medium Impact BES Cyber Systems. The [redacted] personnel stored the relay documents on corporate network drive locations and local drives on compa[redacted] laptops that were not identified and authorized as BES Cyber System Information (BCSI) repositories. The relay documents were also exchanged via e-mail between [redacted], [redacted] Applications, and Transmission Maintenance Center personnel as a part of performing relay maintenance activities. These [redacted] employees had authorization to view and obtain Medium Impact BES Cyber System (relay) shared account passwords in the [redacted] BCSI repository. However, t[redacted]mproper storage and transmis[redacted]a e-mail of this [redacted] these [redacted] out of [redacted] total personnel in [redacted] did not comply with [redacted] documented NERC CIP Information Protection Procedure [redacted]

As part of the [redacted] review in [redacted], [redacted] main[redacted]t of all users that can [redacted] then potentially create relay test sheets through the Transmission Subs[redacted] database. On January 20, 2017, an internal review was initiated working with all users with the ability to create relay test sheets informing them of the issue and asking them to verify if any instances of similar non-compliance had taken place in [redacted]. [redacted] received responses from all users; [redacted] responses led to instances of possible non-compliance with the NERC CIP-011-2 Standard and [redacted] Information Protection Program.

[redacted]

As part of mitigating activities, [redacted] personnel were unable to provide an exact number of the relay test sheets after the fact as many individuals did not keep an accurate count of BCSI documentation while they were purging network and local drives, and e-mails. The exact number of associated [redacted] medium impact substations and specific device passwords impacted in this issue is unknown. All CIP relay passwords that were contained in historical versions of these test sheets were changed prior to July 1, 2016, and many had been changed since July 1, 2016 through a rotational annual password change process. [redacted] It is not feasible to perform annual password change requirements all at one time; therefore, [redacted] personnel change batches of passwords throughout the year. This limited the number of in-scope relay test sheets that would have contained current passwords and still be considered BCSI. It is estimated that around [redacted] relay test sheets were involved in this issue for [redacted] About [redacted] of the relay sheets were stored in restricted SharePoint or network drives and about [redacted] were saved to employee network drives. A much smaller number of those, approximately [redacted], were e-mailed without the proper encryption protections.

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

The root cause of this issue was the individuals and business units involved in this issue failed to fully implement new [redacted] CIP-011-2 procedures during the transition to CIP V5 compliance. Prior to CIP V5 compliance, relay test sheets were not identified as BSCI or treated as Confidential information because the Substation devices they were associated with were also not in-scope of the CIP Standards yet under Version 3. Many transmission relays became Medium Impact BES Cyber Systems in transition to the CIP V5 Standards. The associated relay test sheet became BSCI because some contain a shared account password used to access a shared account when physically at the device.
Up until the effective date of CIP V5 on July 1, 2016, it was common practice for [redacted] Engineers to share and store relay test sheets for business purposes when personnel needed to go into the field an access devices in the switch houses. During the transition to CIP V5 compliance, relay test sheets containing BCSI associated with these newly commissioned Medium Impact assets were not scrubbed from these locations as of July 1, 2016, and some individuals failed to implement new processes for handling and storing BCSI at that time.

However, there was no known harm that occurred as a result of this issue.

Attachments ()

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

These [redacted] personnel [redacted] saved the relay test sheets to their personal network drive, e-mailed them, or upload[redacted]em to a[redacted] protected SharePoint site. [redacted] These groups used the relay test sheets as a part of their normal job functio[redacted]f these storage locations were considered at the time [redacted]zed and identified BCSI repositories, all of the stora[redacted]locations restricted access and use to personnel authorized for access to the information that was originally obtained from the Transmission Substations [redacted] database. [redacted]

Upon discovery, the folder structures for [redacted] Applications, [redacted] an[redacted]h group [redacted]; if it was found, the file was deleted or moved to an auth[redacted]d r[redacted]tory. In this search, all settings files found were reviewed for BCSI and any passwords that were found were deleted from the file. There was also one file found on the [redacted] s[redacted]r, for which [redacted] Operations Compliance worked with [redacted] IT to use a [redacted] tool to search [redacted] email servers for all instances of the known e-mail with a spreadsheet attachment containing shared passwords, and deleted all discovered instances of the message – which included all [redacted] server sent items, inboxes, deleted items, recoverable items, etc. [redacted]

To prevent future recurrence of inadvertent downloading of shared account passwords, [redacted] updated configuration [redacted] within the [redacted] database application where these shared ac[redacted]t passwords are stored to remove shared passwords fr[redacted] default export of Substation device information. Asset owners of the Substations database [redacted] and managers of personnel with the ability to view passwords in the database conducted a review to determine if the number of personnel with access to passw[redacted]o reduce the likelihood of recurrence. [redacted]

As pa[redacted]extent of condition review by [redacted] Operations Compliance, all [redacted] personnel and [redacted] person[redacted]l with th[redacted]bility to view or ac[redacted]device passwords in [redacted]at there were no additional instances of improper storage [redacted]n of this BCSI.

As part of the [redacted] CIP Prod[redacted]e[redacted]nual, [redacted] has implemented the [redacted], CIP Information Protection Program to address CIP-011-2 R1, which [redacted] BES Cyber System Information shall be stored in a controlled access environment designated as a BCSI repository to ensure it is protected." Additionally, "unencrypted BES Cyber System Information (BCSI) should not be transmitted using co[redacted]at[redacted]mail systems. Links to access contro[redacted]d BCSI repositories should be provided in e-mail whenever possible. However, in the event that [redacted] mailed, the BCSI must be contained within a file attached to the e-mail message, and the file must be encrypted using an approved encryption tool listed on the HW/SW Product Catalog, such as, but not limited to, [redacted]." [redacted]

Test engineers use relay test sheets to perform routine maintenance on substation relays. The relay test sheets found in ques[redacted]f this issue contained a shared level II password for CIP relays that would allow electronic access that could be used to alter the configuration of a relay if the person was physically standing at the relay within the substation PSP. The presence of the shared password in these relay test sheets elevates them to the classification of BCSI per the criteria defined in [redacted].

The Substations organizations across [redacted] operating companies also developed in response to this issue a Substations Field Guide on 'How to Handle BES Cyber System Information' which is to be used to provide more easily discernable guidance on how to handle BES Cyber System Information for [redacted] Substations field personnel. These steps are an extension of the [redacted]

This issue was not discovered through a formal internal controls process, but rather through the extent of condition review of another self-reported issue originating in [redacted]

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:

Description of Mitigating Activities:
1) [redacted] will require managers to review all individuals with [redacted] role in [redacted] to determine if the scope of individuals with this role can be reduced to further restrict access to passwords where needed. Completed 3/31/17.
2) [redacted] will draft a [redacted] specifically addressing the proper protection and secure handling of BES Cyber System Information, including storage, transit, and use, where applicable, and new request processes and secure storage of passwords. Completed 4/18/2017
3) [redacted] and [redacted] Transmission Compliance will conduct retraining of all personnel with [redacted] role in [redacted] on the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and train personnel on Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use. Completed 4/25/2017
4) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Completed 5/15/2017

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

[redacted] has conducted retraining with the personnel with access privileges in the Transmission [redacted] database to view and download device passwords to reinforce new CIP procedures around properly storing BCSI in designated and authorized BCSI repositories, as well as the Information Protection Program requirements outlining the requirements around how to properly e-mail BCSI internally, when necessary. Additionally, [redacted] administrators have implemented additional technical controls within the [redacted] database to remove the potential of inadvertently exporting relay test sheets that contain device shared account passwords. Personnel in all of the OPCOs with the ability to access these passwords were also trained on these new [redacted] processes.

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:

5/19/2017

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

Closure Package to SERC

Milestone Completed (Due: 5/19/2017 and Completed 5/15/2017)

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

[redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.

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):

(i) There are no known additional risks or impacts to the BPS while the actions in this mitigation plan are being completed.
(ii[redacted] does not plan to implement additional actions that would increase risks to the reliability of the BPS as part of this mitigation plan.

[redacted] assesses this issue posed a minimal actual risk, and not a serious or substantial risk to the reliability of the bulk electric system. Unauthorized storage and disclosure of the shared account passwords in question could have aided in the potential of unauthorized electronic access if personnel also had authorized physical access to the PSPs where these devices are located. Personnel would have had to obtain shared relay passwords in combination with physical access, relay terminal software, and relay usage knowledge to be capable of changing device settings, flash firmware, or close contacts leading to a trip of a breaker on the bulk power system. Accessing the Medium Impact BES Cyber System relays remotely was not possible using only the shared account passwords contained in these relay test sheets [redacted] IRA therefore was not possible with the shared account passwords alone contained in the relay test sheets. Alternatively, knowledge of the device passwords, in combination with authorization for Interactive Remote Access, could allow a user the ability to change device passwords and potentially temporarily lock others out of the system. Unauthorized changes of device passwords in combination with other potential device setting changes could affect the way a device was designed to operate.

This issue poses a minimal actual risk, and not a serious or substantial actual risk to the bulk power system. The spreadsheets in question were stored on a business unit shared drive, but the location these spreadsheets were temporarily stored in was not on the designated list of BES Cyber System Information repositories as required by [redacted].
All of the individuals that received via e-mail a file containing the shared account passwords in question did have current authorization to view or access those passwords in [redacted], and all of these employees do have active authorization for other electronic and/or physical access to CIP areas or systems, which requires a valid, compliant background check and the completion of annual NERC CIP training. [redacted] personnel control access to shared drives through [redacted] groups that are restricted to authorized users within their business units. BCSI provided during the INPO audit was stored on a SharePoint site restricted to authorized transmission and nuclear personnel only. For the relay test sheets hat were e-mailed, they were sent over the secured [redacted] exchange server to other internal personnel. Although the files were not encrypted individually, they were transmitted via an encrypted network.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitiga ion 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 will minimize the probability of future violations of the same requirements by providing additional clarifying instructions in a new [redacted] specifically addressing the proper protection and secure handling of BES Cyber System Information, including storage, transit, and use, and by retraining of all personnel with [redacted] role in [redacted] on the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future.
As noted in the originally submitted self-report, [redacted] has completed the following actions to prevent future recurrence:
1) [redacted] will require managers to review all individuals with View Passwords role in [redacted] to determine if the scope of individuals with this role can be reduced to further restrict access to passwords where needed. Completed 3/31/17.
2) [redacted] will draft a [redacted] specifically addressing the proper protection and secure handling of BES Cyber System Information, including storage, transit, and use, where applicable, and new request processes and secure storage of passwords. Completed 4/18/2017
3) [redacted] and [redacted] Transmission Compliance will conduct retraining of all personnel with [redacted] role in [redacted] on the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and train personnel on Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use. Completed 4/25/2017

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 SERC and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
  - I am [redacted] of [redacted]
  - I am qualified to sign this Mitigation Plan on behalf of [redacted]
  - I understand [redacted] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendixe 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 SERC and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

SERC Single Point of Contact (SPOC)

VIEW MITIGATION PLAN CLOSURE: CIP-011-2 (MITIGATION PLAN CLOSURE COMPLETED)

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

This item was signed by [redacted] on 9/4/2018

This item was marked ready for signature by [redacted] on 8/31/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC 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.	SERC2017-402689	SERC2017017564

Date of completion of the Mitigation Plan:

[redacted]

Closure Package to SERC

Milestone Completed (Due: 5/19/2017 and Completed 5/15/2017)
Attachments (0)

[redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.

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

Description of Mitigating Activities:
1) [redacted] will require managers to review all individuals with [redacted] role in [redacted] to determine if the scope of individuals with this role can be reduced to further restrict access to passwords where needed. Completed 3/31/17.
2) [redacted] will draft a [redacted] specifically addressing the proper protection and secure handling of BES Cyber System Information, including storage, transit, and use, where applicable, and new request processes and secure storage of passwords. Completed 4/18/2017
3) [redacted] and [redacted] Transmission Compliance will conduct retraining of all personnel with [redacted] role in [redacted] on the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and train personnel on Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use. Completed 4/25/2017
4) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Completed 5/15/2017

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

[redacted] has conducted retraining with the personnel with access privileges in the Transmission [redacted] database to view and download device passwords to reinforce new CIP procedures around properly storing BCSI in designated and authorized BCSI repositories, as well as the Information Protection Program requirements outlining the requirements around how to properly e-mail BCSI internally, when necessary. Additionally, [redacted] administrators have implemented additional technical controls within the [redacted] database to remove the potential of inadvertently exporting relay test sheets that contain device shared account passwords. Personnel in all of the [redacted] with the ability to access these passwords were also trained on these new [redacted] processes.

Description of the information provided to SERC for their evaluation *

Milestone 1
[redacted] This document depicts email confirmation that [redacted] and [redacted] reviewed all individuals with access to shared passwords in [redacted] to determine if the scope of individuals with this role can be reduced to further restrict access to passwords, where needed, by 3/31/2017; where the scope of personnel could be reduced, a screenshot has been included from the [redacted] Access Management Application ([redacted]) showing a revocation of authorization for the roles o [redacted].

Milestone 2:
[redacted] This document depicts the [redacted] developed specifically to reinforce the proper protection and secure handling of BES Cyber System Information, including storage, transit, and use, where applicable, and new [redacted] processes to ensure the secure storage of passwords. The [redacted] was approved by Substations Management on 4/18/2017.

Milestone 3:
[redacted] This document shows the time, date, and attendees present at various [redacted] training sessions, as well as an [redacted] training session, which included training regarding the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use.
[redacted]; This document shows the distribution on 4/25/2017 of re-training materials regarding the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use to [redacted] personnel, as well as [redacted] personnel with access to [redacted] shared passwords.
[redacted] This document shows the attendees present at [redacted] training session on 4/25/17, which included

training regarding the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use.

[redacted] This document shows the distribution on 4/6/2017 and attestation of completion on 4/22/2017 of re-training materials regarding the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use to the one [redacted] employee with access to [redacted] shared passwords.

[redacted] This powerpoint presentation shows the content of retraining materials used by each operating company group conducting reinforcement training with individuals with access in [redacted] to shared passwords. This training covered the configuration changes in [redacted] to prevent the inadvertent downloading of device passwords in the future, and Substation procedures on protecting and securely handling BES Cyber System Information, including storage, transit, and use.

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.