

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:

- The decision to move the visitor log book to the outside of the West door was a mitigation step to securely manage the entrance to the PSP with one location.
- A communication was sent out about the changes on 7/27/16 to direct reports of the manager of system operations in [REDACTED] as well as to those with offices in the [REDACTED]
- Signs were posted at the PSP which acted as a secondary security notification for those who rarely enter the [REDACTED]. The signs were to further clarify the actions to be taken with regard to the visitor logs.

Provide details to prevent recurrence:

- Due to the violations that have occurred around the Visitor/Escort events, a new root cause is being performed to identify additional actions to help prevent recurrence in addition to the previously implemented item.
- Regarding the [REDACTED] a communication will be sent out to [REDACTED] who have access to the [REDACTED]
- An evaluation will be done with regard to the placement of the signs.

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

11/30/2016

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:

The Potential Impact to the Bulk Power System is minimal because the sites being mentioned continue to be secured and monitored on a 24 hour, 7 days a week basis. The visitors were continuously escorted the entire time they were in the PSP.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation. Additionally, the visitors were continuously escorted the entire time they were in the PSP.

Additional Comments:

[REDACTED] was attempting to comply in good faith with the application NERC reliability standard at issue in this instant alleged violation situation by having the Visitor Log in place at the [REDACTED] as well as training, and reviews of Visitor Logs.

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.)

Post On-site Audit/Off-site Audit/Spot Check/Investigation Screening Worksheet

Prepared By: [REDACTED]

Submittal Date: [REDACTED]

Compliance Monitoring Method (On-site Audit, Off-site Audit, Spot-Check, or Investigation):
On-site Audit

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

Registered Entity Contact Information:
[REDACTED]

Standard: CIP-006-6

Requirement: R2

Sub Requirement(s): 2.2

Function(s) Applicable to Possible Violation:

[REDACTED]

Date violation occurred: 8/2/2016

Date violation discovered (Exit Presentation Date): [REDACTED]

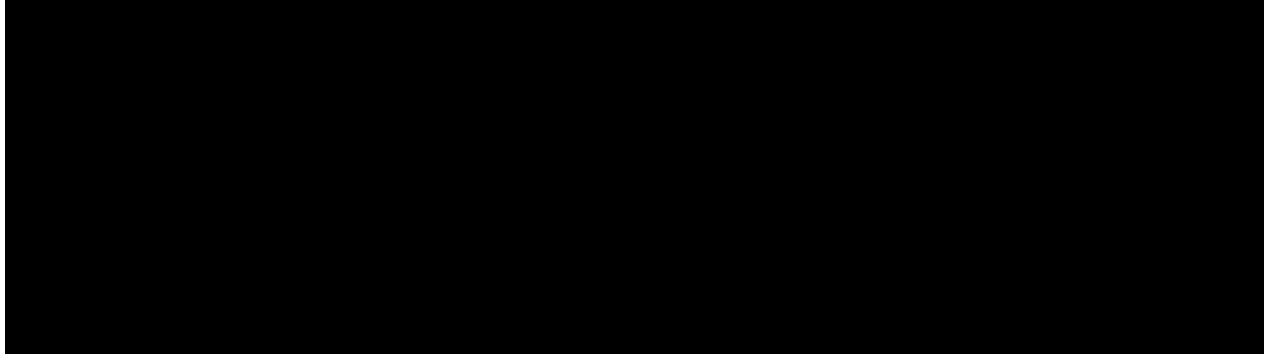
Is the violation still occurring? Yes No

Are mitigating activities (including details to prevent reoccurrence) in progress or completed? Yes No

If yes, Provide description of Mitigating Activities:

Date Mitigating Activities are expected to be completed or were completed:

Detailed explanation and cause of violation: Visitors to various PSPs forgot to either log out or enter the name of their escort in the Visitor Log.



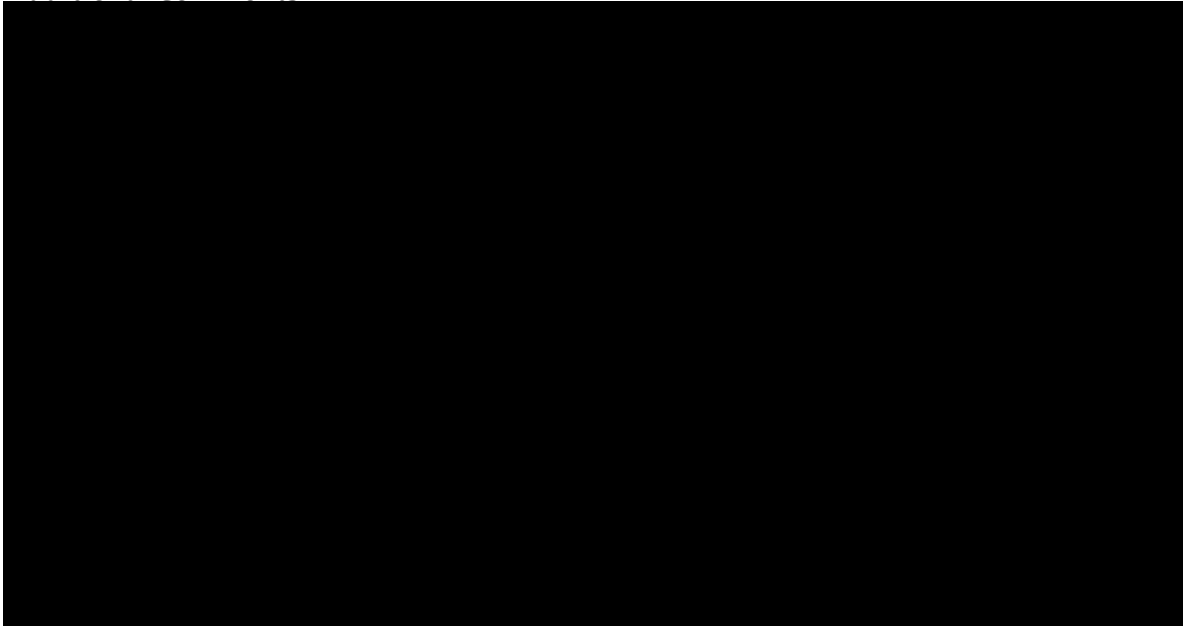
Potential Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

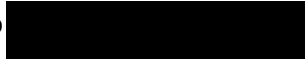
Actual Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

Detailed description of Potential Risk to Bulk Power System: If visitors are not logged properly either in a PACS or on written logs due to weak controls or personnel indifference then unauthorized persons might be allowed entrance with little regard as to why they are there or whether they are even escorted.

Detailed description of Actual Risk to Bulk Power System: Each visitor was escorted by an authorized person while within the PSP. Video evidence documents the time of exit and the escort present.

Additional Comments:



Please complete the form as completely as possible and email to 

This item was submitted by [REDACTED] on 9/12/2017

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: CIP-006-6

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.2.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

5/5/2015

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: Yes

If yes, indicate which Region(s):

[REDACTED]

Date Reported to Region(s):

[REDACTED]

Date Possible Violation was discovered: 11/30/2016

Beginning Date of Possible Violation: 11/30/2016

End or Expected End Date of Possible Violation: 12/31/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

In accordance with CIP 006-5 R2.2 that states: "Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances."; [REDACTED] maintains manual visitor logs to document the entry and exit from Physical Security Perimeters. These logs include all of the above required fields.

On November 28, 2016, [REDACTED] completed an enterprise Common Cause Analysis (CCA) to address NERC CIP visitor logging violations of CIP-006, R2.2. The scope of this analysis covered self-reported events between June 2015 and September 2016. As a result, there are two possible violations that were not included in the enterprise analysis. Additionally, the corrective actions from the CCA were not yet completed and therefore could not have prevented these possible violations. These possible violations include the following:

PV # Event Title
[REDACTED] October 2016 Visitor Log Failures

A Direct Cause Analysis (DCA) was conducted to assess these possible violations that were not included in the CCA and to determine whether the causes of those issues were previously covered in the enterprise CCA. The DCA has not identified any unique or new causes that were not already identified in the enterprise CCA. As a result, the corrective actions in the existing mitigation plan will address each of the visitor log failures covered in this DCA.

The cause of these issues are because Physical Security Procedure was not followed. Employees and contractors did not correctly fill in all of the entries on the Visitor Log form, and the Escorts did not make sure that all entries were complete on the Visitor Logs. However, the visitors were not left unescorted the entire time they were in the PSP.

This self report covers two possible violations:

Possible Violation #1. - October Visitor Log Failures

Visitor Log entries for October contained possible violations for personnel without authorized unescorted access to PSPs. Of these Possible Violations, there were 1 self report violation. The violation occurred in the following region: The location of where the violation occurred was the The violation occurred in the following field: "Last Time Out". The escort who was responsible was from the following business area:

Sites in scope:



Possible Violation #2. - November Visitor Log Failures

Visitor Log entries for November contained possible violations for personnel without authorized unescorted access to PSPs. Of these Possible Violations, there were 1 self report violation. The violation occurred in the following region: The location of where the violation occurred was the The violation occurred in the following field: "Last Time Out". The escort who was responsible was from the following business area:

The Extent of Condition analysis and an enterprise Common Cause Analysis that was performed uncovered visitor log violations across all jurisdictions. This information has been documented in the Common Cause Analysis that was performed on 11/28/2016 and that covered the period from June 2015 to September 2016. It is part of the filed with

The cause of these issues is Transmission's physical security procedures were not followed. Employees and contractors did not correctly fill in all of the entries on the Visitor Log form, and the Escorts did not make sure that all entries were complete on the Visitor Logs. However, the visitors were not left unescorted the entire time they were in the PSP.

The direct and contributing causes of these possible violations are as follows:

Cause ID 1- Misunderstanding of Policy and Procedure by Infrequent Escorts or Visitors (CCA - Cause 1)

- Inadequate training for employees and contractors on proper logging in and out including how to address abnormal circumstances.
- a. It was found that the Computer Based Training (CBT) for the PSP did not reflect all of the knowledge necessary to adequately perform the role of escort. Little information was available on log completion and the variety of different possible logging scenarios, and little information was available on what signage to expect.
- b. Proficiency of the student (contractor or employee) studying the material was not effectively demonstrated at the completion of the CBT. In the existing CBT, a student can select all wrong answers and still successfully complete the course.
- c. There is a lot of information to retain in this training for someone new to NERC CIP. In addition to learning about roles and responsibilities required with authorized unescorted access, there are a lot of terms that are used in the training that are new to contractors and other employees such as field personnel who infrequently enter PSP.
- d. There is no review of scenarios that have or would result in a NERC CIP violation
- e. While there is one image of completed log, there are no images or training showing what an incomplete log looks like and why it would be a NERC CIP violation.
- Logging techniques unclear when badges of individuals with existing authorized unescorted access fail to work.
 - a. Although the mentions what to do in the event of a badge not working, it isn't clear to individuals who have authorized unescorted access that if their badge isn't working for any reason or if they do not have their badge with them, then they are to be treated as a guest and must log in and have an escort.
- Lack of effective education and socialization about NERC CIP logging requirements and potential consequences throughout the enterprise.
 - a. While the importance of NERC CIP, potential consequences from violations, and actual violations are socialized at leadership level in it isn't effectively socialized and visible to all levels of the organization and across the enterprise. Many employees are unaware of the importance of insuring proper logging is completed.
- Lack of effective communication between escort and visitor regarding expectations of each while in the PSP.
 - a. There is no procedure or process that requires an escort to review the roles and responsibilities of the escort and the visitor when entering into a PSP.
 - b. The escort is not required to have their visitor peer check them and review the log for accuracy prior to and after exiting PSP.

Cause ID 2 -Lack of Process Controls by Infrequent Escorts or Visitors (CCA - Cause 2)

- Ineffective barriers in place to prevent visitors from leaving without logging out.
- Concept of multiple logs makes appropriate log keeping control difficult to maintain.
 - a. Having multiple access points and logs increases the likelihood that a visitor will exit the PSP without logging out.
- Lack of fundamental human performance techniques such as 2-minute drill and peer checking prior to and when exiting the PSP.
 - a. Currently, there is no requirement that escorts utilize human performance techniques to reduce the likelihood of a logging error.

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

The following milestones have been completed or will be completed as part of the enterprise visitor management mitigation plan

MS 1 - Project Management Process Updates
Update project management processes to better define the engagement points with NERC CIP facility stakeholders including NERC
Completed 6/15/2015

MS 2 - Calculate Monthly Visitor Log Failure Rate
Track, monitor and analyze enterprise visitor log errors and failures to determine business area and regional failure rates.
Completed 9/1/2015

MS 3 - Develop Escort/Authorizer Roles Responsibilities and Expectations
Update to include Escort/Authorizer Roles, Responsibilities and Expectations.
Completed 11/30/2015

MS 4 - Visitor Log Template Enhancements
Redesign manual visitor log template to make it more intuitive for the escort and eliminate human performance issues.
Completed 12/18/2015

MS 5 - Include Escort/Authorizer Roles and Responsibilities with Each Visitor Log
Include Escort/Authorizer Roles and Responsibilities with Each Visitor Log to eliminate human performance issues.
Completed 12/31/2015

MS 6 - Approve Updated Visitor Log Template

Obtain approval of enterprise manual visitor log template from business area approvers and CIP Senior Manager
(Completed 1/18/2016)

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

MS 7 - Implement Updated [REDACTED] Visitor Log Template at All PSPs
Updated manual enterprise visitor logs are rolled out to NERC CIP sites
(Completed 3/7/2016)

MS 8 - [REDACTED] Training Modification - Escort Responsibilities Edit and disseminate the [REDACTED] 2016 training module to include appropriate human performance behaviors for escorting a visitor and prohibiting others from entering the PSP after a successful badge scan.
Completed 3/31/2016

MS 9 - Calculate [REDACTED] Monthly Visitor Log Failure Rate
Perform detailed analysis of human performance trends for enterprise visitor log error rates for April, 2016.
Completed 5/31/2016

MS 10 - Update [REDACTED] Policy for Visitor Log Editing
Update [REDACTED] to reflect policy for editing manual visitor logs.
Completed 6/6/2016

MS 11 - Calculate [REDACTED] Monthly Visitor Log Failure Rate
Perform detailed analysis of human performance trends for [REDACTED] log error rates for July 2016.
Completed 9/1/2016

MS 12 - Calculate [REDACTED] Monthly Visitor Log Failure Rate
Perform detailed analysis of human performance trends for [REDACTED] log error rates for August, 2016.
Completed 9/30/2016

MS 13 - Training & Awareness - Site Specific Training for [REDACTED]
Develop and deliver site specific training and materials with floor plans, designated access points, signage and processes for all [REDACTED] to all personnel with unescorted CIP access to [REDACTED]
Completed 11/1/2016

MS 14 - Implement Visitor Management Coaching Guidelines within the [REDACTED]
Implement Visitor Management Coaching Guidelines within the [REDACTED]
Completed 11/15/2016

MS 15 - Executive Communication - Changes to Access Points to PSPs
Develop and deliver executive communication regarding changes to the ingress/egress policy and process at all high impact [REDACTED] to all personnel with unescorted CIP access to high impact [REDACTED]
Completed 11/18/2016

MS 16 - Reduce Number of Individuals with Authorized Access To [REDACTED]
Perform analysis of all individuals with authorized unescorted access to a PSP and develop more strict criteria for authorizing such access.
Completed 11/29/2016

MS 17 - [REDACTED] Pilot Implementation
Perform a pilot implementation of an [REDACTED] within a secure office area in the [REDACTED]
Completed 12/9/2016

MS 18 - [REDACTED] Training & Awareness - Access Process for Authorized Individuals w/Malfunctioning Badge
Develop and deliver [REDACTED] communication to address the process for individuals with authorized unescorted access in the event their badge malfunctions or is damaged.
Completed 2/28/2017

MS 19 - Supplemental Evidence to Document Last Time Out for Visitors
Develop and implement a standard procedure for the gathering and use of video evidence to supplement a manual visitor log in the event the last time out field is not completed.
Completed 2/28/2017

MS 20 - Implement Visitor Management Coaching Guidelines in IT Organization
Implement Visitor Management Coaching Guidelines within the IT Organization.
Completed 3/31/2017

MS 21 - Human Observation at [REDACTED] Access Points
[REDACTED] will post a Security Officer at the primary access point at each of its [REDACTED] active High BES Control Centers; develop and provide Post Order Instructions for each site, and ensure all Officers assigned to the posts have reviewed the Post Orders and understand the responsibilities.
Completed 3/31/2017

MS 22 - Reduce Access Points to PSPs
Perform operational analysis to reduce the number of all current and future access points to each PSP. Evaluate each access point for potential human error traps including visitor log book location, and appropriate signage.
Completed 4/30/2017

MS 23 - [REDACTED] Modification - Add Knowledge Retention Test to CBT
Enhance existing [REDACTED] CIP-004 training materials to include a knowledge retention test that must be repeated until all test questions are answered correctly.
Completed 5/31/2017

MS 24 - [REDACTED] Training Modification - Add Visitor Management Scenarios to CBT
Enhance existing CIP-004 training materials to include operational scenarios an escort will encounter including escorting groups, badge failures, PACS outages, etc.
Completed 5/31/2017

MS 25 - [REDACTED] Training Modification - Add Examples of Properly Completed Visitor Logs to CBT
Enhance existing [REDACTED] CIP-004 training materials to include examples of a properly completed visitor log entry.
Completed 5/31/2017

MS 26 - Training Modification - Add Clarity for Visitor Logging During PACS Outage
Enhance existing [REDACTED] CIP-004 training materials to include clarity for appropriate actions in the event of a PACS outage or forgotten or malfunctioning badge.
Completed 5/31/2017

MS 27 - Develop Procedure for PSP Pre-Entry Drill
Develop a Procedure for Pre-Entry Drill to be performed prior to entering a PSP to review the roles, responsibilities and human performance expectations of the escort and visitor.
Completed 6/1/2017

MS 28 - [REDACTED] Visitor Log Procedure Enhancements
Correct contradictory language in [REDACTED] procedure relating to how to fill out the "company/affiliation" field on the visitor log.
Completed 6/30/2017

MS 29 - Perform Training for the PSP Pre-Entry Drill
Performing training, to all personnel with unescorted CIP access, on Procedure for PSP Pre-Entry Drill to be performed prior to entering a PSP to review the roles, responsibilities and expectations of the escort and visitor.
Completed 7/31/2017

MS 30 - Implement Procedure for PSP Pre-Entry Drill

Implement a Procedure for PSP Pre-Entry Drill to be performed prior to entering a PSP to review the roles, responsibilities and expectations of the escort and visitor.

Completed 7/31/2017

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

MS 31 - Site Surveys for [REDACTED] Production Implementation

Conduct site surveys for [REDACTED] deployment at [REDACTED]

Completed 7/31/2017

MS 32 - [REDACTED] Production Implementation at [REDACTED]

[REDACTED] Production Implementation at [REDACTED]

Completed 8/30/2017

MS 33 - [REDACTED] Production Implementation at [REDACTED]

Implementation of the [REDACTED] solution at CIP [REDACTED]

Scheduled 10/30/2017

MS 34 - Develop Stakeholder Awareness Process for PSP Changes

Develop and implement [REDACTED] Stakeholder Awareness Process for PSP Changes".

Scheduled 10/30/2017

MS 35 - Clarify PSP Exterior Signage

Deploy [REDACTED] standard signage at all PSPs access points that describe the roles, responsibilities and expectations of escorts.

Scheduled 10/31/2017

MS 36 - Implement PSP Interior Signage

Implement PSP Interior signage (new sign) that reinforces the necessity to complete the visitor log accurately

Scheduled 10/31/2017

MS 37 - Clarify PSP Signage for Tailgating Policy

Remove existing PSP signage and replace with standard PSP signage for tailgating policy

Scheduled 10/31/2017

MS 38 - Communicate Monthly [REDACTED] Visitor Log Failure Rates

Communicate the performance metrics from the monthly [REDACTED] log analysis to stakeholders and leadership throughout [REDACTED] each month

Scheduled 12/31/2017

Provide details to prevent recurrence:

* [REDACTED] Leadership Oversight and Review—[REDACTED] will perform analysis and develop visitor log and escort human performance metrics on a monthly basis. These metrics will be reported to senior leadership across all [REDACTED] on a quarterly basis. This activity is designed to provide persistent visibility to senior leadership throughout the enterprise regarding human performance and operational discipline and to enforce accountability in all [REDACTED] business areas.

* Reduce Access Points to PSPs at [REDACTED]—[REDACTED] will reduce the number of ingress points to all PSPs at [REDACTED] to eliminate unnecessary access points and the number of visitor logs placed in the PSPs. This activity is designed to address human performance issues at NERC CIP high impact PSPs by reducing human error traps associated with visitor management and escort responsibilities.

* [REDACTED] Manual Visitor Log Enhancements—[REDACTED] will reassess its [REDACTED] log template to address problematic areas that contribute to human performance failures. Considerations include removing fields to simplify the visitor logging process and reformatting the form to emphasize escort responsibilities. This activity will make the visitor log more intuitive to address human performance failures and by reducing error traps.

* Compute [REDACTED] Manual Log Failure Rates—[REDACTED] will calculate the manual logging failure rates across the [REDACTED] within all [REDACTED] business areas. The degree of human performance failure in each region will be identified and communicated on a monthly basis. This activity includes leadership reinforcement of human performance and operational discipline expectations with employees utilizing our Visitor Management Coaching Guidelines.

* [REDACTED] Solution—[REDACTED] will implement a technology solution for visitor logging at all NERC CIP PSPs across the enterprise. This solution is designed to address human performance failures and to reduce common human error traps associated with the current paper solution.

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

12/12/2017

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:

The potential impact to the Bulk Electric System (BES) could be moderate if the visitors were not continuously escorted while they were within the PSP. However, the visitors were continuously monitored and the site is secured and monitored on 24x7. As a result, it is concluded the potential impact to the BES is minimal.

Provide detailed description of Actual Risk to Bulk Power System:

The actual impact to the Bulk Electric System (BES) is minimal because the individual (escort) responsible for the visitors was in positive control of the visitors and their activities while within the PSP. As a result, no misoperations, emergencies, or other adverse consequences to the Bulk Electric System occurred due to this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation by having the visitor log in place at the [REDACTED] as well as training and reviews of Visitor Logs.

An Extent of Condition showed that this condition exists within other groups. As a result of these issues, a Common Cause Analysis was performed and a Mitigation Plan

developed.

**PRIVILEGED 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.)

This item was submitted by [REDACTED] on 9/12/2017

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: CIP-006-6

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.2.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

5/5/2015

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: Yes

If yes, indicate which Region(s):

[REDACTED]

Date Reported to Region(s):

6/10/2015

Date Possible Violation was discovered: 5/11/2017

Beginning Date of Possible Violation: 4/18/2017

End or Expected End Date of Possible Violation: 4/18/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP-006-5; R2.2, [REDACTED] is obligated to log visitor's entry into and exit from the Physical Security Perimeter (PSP) that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor.

On April 18th, 2017 a Contractor (with NERC CIP Access) and an additional Contractor (No NERC CIP Access) arrived at [REDACTED] at 7:04am. At this time the log book was correctly filled out for their initial entry into the PSP.

At approximately 3pm, these two contractors were requested to assist in a medical emergency, in the switchyard, outside of the PSP. After assisting the injured party and directing Emergency Services to the scene, the contractors returned to the [REDACTED] control house (PSP), gathered their tools, and left the facility. At this time, the last time out section of the visitor log was not filled out.

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Immediate Mitigating Actions Taken:

1. [Redacted] to deliver a communication to all [Redacted] Employees highlighting a recommended HP action to assist in log book completion at [Redacted] (Escort attaches vehicle keys to log book) - Complete
2. Verbally reinforce Corrective Action #1 during a staff meeting in June 2017. [Redacted] Complete
3. Verbally reinforce Corrective Action #1 during a staff meeting in June 2017. [Redacted] Complete
4. Verbally reinforce Corrective Action #1 during a staff meeting in June 2017. [Redacted] Complete
5. Verbally reinforce Corrective Action #1 during a staff meeting in June 2017. [Redacted] Complete
6. Verbal Communication issued to [Redacted] Employees stressing the importance of securing site - Complete

Provide details to prevent recurrence:

In addition to mitigating activities previously filed with Mitigation Plan [Redacted] has taken or plans to take with respect to this issue include the following:

1. [Redacted] to deliver a communication to all [Redacted] Employees highlighting a recommended HP action to assist in log book completion at [Redacted] (Escort attaches vehicle keys to log book) - Complete
2. Verbally reinforce Corrective Action #1 during a staff meeting in June 2017. [Redacted] Complete
3. Verbally reinforce Corrective Action #1 during a staff meeting in June 2017. [Redacted] Complete
4. Verbally reinforce Corrective Action #1 during a staff meeting in June 2017. [Redacted] Complete
5. Verbally reinforce Corrective Action #1 during a staff meeting in June 2017. [Redacted] Complete
6. Verbal Communication issued to [Redacted] Employees stressing the importance of securing site - Complete
7. [Redacted] to deliver a reinforcement communication to all [Redacted] employees stressing the importance of visitor logging.
8. Develop a checklist to facilitate a site by site review of [Redacted] to ensure that signage, reminders, and HP tools are in place to reinforce the importance of visitor logging. Checklist to include section to document the non-primary doors slated for conversion to (alarmed) exit-only.
9. Once the updated [Redacted] and Mitigation Plan [Redacted] have been completed, [Redacted] and [Redacted] Analysts will perform a site by site review to ensure that signage, reminders, and HP tools are in place to reinforce the importance of visitor logging and document the non-primary doors at each site that will be converted to (alarmed) exit only.
(Medium Impact Sites with ERC in [Redacted])
10. Convert non-primary doors identified in Corrective Action #9 to Emergency Exit only. Install Emergency Exit sign package.
11. Once the updated [Redacted] and Mitigation Plan [Redacted] have been completed, [Redacted] and [Redacted] Analysts will perform a site by site review to ensure that signage, reminders, and HP tools are in place to reinforce the importance of visitor logging and document the non-primary doors at each site that will be converted to (alarmed) exit only.
(Medium Impact Sites with ERC in [Redacted])
12. Convert non-primary doors identified in Corrective Action #11 to Emergency Exit only. Install Emergency Exit sign package.
13. Once the updated [Redacted] and Mitigation Plan [Redacted] have been completed, [Redacted] and [Redacted] Analysts will perform a site by site review to ensure that signage, reminders, and HP tools are in place to reinforce the importance of visitor logging and document the non-primary doors at each site that will be converted to (alarmed) exit only.
(Medium Impact Sites with ERC in [Redacted])
14. Convert non-primary doors identified in Corrective Action #13 to Emergency Exit only. Install Emergency Exit sign package.
15. Once the updated [Redacted] and Mitigation Plan [Redacted] have been completed, [Redacted] and [Redacted] Analysts will perform a site by site review to ensure that signage, reminders, and HP tools are in place to reinforce the importance of visitor logging and document the non-primary doors at each site that will be converted to (alarmed) exit only.
(Medium Impact Sites with ERC in [Redacted])
16. Convert non-primary doors identified in Corrective Action #15 to Emergency Exit only. Install Emergency Exit sign package.

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

12/12/2017

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:

The potential impact to the Bulk Electric System (BES) could be moderate if the visitors were not continuously escorted while they were within the PSP. However, the visitors were continuously monitored and the site is secured and monitored on 24x7. As a result, it is concluded the potential impact to the BES is minimal.

Provide detailed description of Actual Risk to Bulk Power System:

The actual impact to the Bulk Electric System (BES) is minimal because the individual (escort) responsible for the visitors was in positive control of the visitors and their activities while within the PSP. As a result, no misoperations, emergencies, or other adverse consequences to the Bulk Electric System occurred due to this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard

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.)

This item was submitted by [REDACTED] on 12/21/2017

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: CIP-006-6

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.2.

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): [REDACTED]

Date Reported to Region or Discovered by Region: 9/12/2017

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: 9/26/2017

Beginning Date of Possible Violation: 9/24/2017

End or Expected End Date of Possible Violation: 9/26/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

The [REDACTED] utilizes [REDACTED] to provide a platform for [REDACTED] and contractors with authorized, unescorted physical access to NERC CIP high and medium Physical Security Perimeters (PSP's) to electronically log visitors who enter and exit the PSPs. Visitor logging information required to be entered into the [REDACTED] includes the date and time of the initial entry and the last exit, the visitor's name, and the name of the escort.

[REDACTED] conducts a weekly review of a report generated by the [REDACTED] tool of all the visitors from the previous week. On September 26, 2017, [REDACTED] discovered and then notified [REDACTED] that a visitor logging error had occurred the morning of September 24, 2017 at the [REDACTED] there had been a failure to log two visitors' last PSP exit. This error occurred due to an [REDACTED] having difficulty logging two visitors into the [REDACTED] system, and rather than entering information for the visitors, the [REDACTED] had mistakenly entered his name into the system twice as being a visitor, after scanning his [REDACTED] Identification Badge which entered him in as the escort. When the visitors exited the PSP the [REDACTED] also had difficulties and did not successfully log the two visitors' exit using the kiosk. The visitors were inside the PSP for approximately one hour.

This event resulted in reporting a Possible Violation Self Report (PVSr) to the [REDACTED] of a compliance violation of NERC Standard CIP-006-6, R 2.2. The Standard requires manual or automated logging of escorted visitor entry into and exit from the PSP that includes the date, the time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Accounting for all visitor activity within a Physical Security Perimeter (PSP) is a core tenant of any cyber security policy, including NERC CIP. Additionally, if no formal record exists of visitors entering and exiting PSPs, there would be no way to perform an after the fact investigation of any potential Cyber Security Incidents. As a result, if an individual without authorized (unescorted) access is not continuously escorted while inside the PSP, and is able to access BES Cyber Systems, the potential risk to the BES could be moderate.

Provide detailed description of Actual Risk to Bulk Power System:

Although the potential impact to the Bulk Electric System is moderate, the actual risk to the BES is low because the individuals (visitors) that were within the [REDACTED] were continuously escorted by an authorized [REDACTED] employee and did not access BES Cyber Systems. As a result, there was no actual impact to the BES caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the BES.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

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.)

This item was submitted by [REDACTED] on 12/21/2017

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: CIP-006-6

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.2.

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: 10/18/2017

Beginning Date of Possible Violation: 10/12/2017

End or Expected End Date of Possible Violation: 10/18/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On Thursday, 10/12/17, an [REDACTED] escorted two painters into the [REDACTED]. At the end of the shift, when the employee and the painters exited the [REDACTED] the employee attempted to sign the visitors out at the [REDACTED] (the employee is CIP badged and therefore not required to log himself in or out). During the sign out process, the [REDACTED] received a message on the kiosk screen that stated "Process Complete", leading him to believe he had successfully logged the visitors out. Later that same evening, a night shift employee logged into the [REDACTED] and noticed that the two painters were still logged in. [REDACTED] initiated.

The software interface from the [REDACTED] stating "Process Complete", led the [REDACTED] to believe his log-out efforts were successfully completed, although additional steps were required to log out the visitors. This was also the first time the individual logged out visitors using the new electronic system. Prior to this event, [REDACTED] personnel were already working to update the [REDACTED] software to make the visitor logout process more intuitive and help prevent similar log out issues they had been experiencing with the new system.

Reviewing the kiosk main screen to ensure all personnel were signed out after completing the logout process would have alerted the employee to the failed attempt and prevented this event from occurring. Also, if the employee was unsure, he could have called the number located at the kiosk to verify the visitors were successfully logged out. Interviews with the employee revealed he was not unsure, and fully believed he had logged the visitors out. This prevented any log out review or verification.

Are Mitigating Activities in progress or completed? 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:

The potential impact to the Bulk Electric System is minimal because the visitors exited the [REDACTED] as required while being escorted. The employee escort attempted, but failed to properly log the visitors out of the system. This failure was noticed early on the next shift, and the appropriate personnel were notified. Immediate actions were taken to post correct directions at the kiosk to aid others in properly logging visitors out until the software upgrades were taken to make the logout process more intuitive and user friendly.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Electric System caused by this possible violation because there were no misoperations, emergencies, or other adverse

consequences to the Bulk Electric System as a result of this possible violation.

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

Additional Comments:

This possible violation was not the result of any intentional action to violate any NERC reliability standard. [REDACTED] personnel were attempting to comply in good faith with the applicable NERC reliability standard in this possible violation event. Software updates have already been complete to upgrade the visitor logout system to help prevent future similar events. [REDACTED] senior management, lower level managers, and direct managers relevant to this situation actively participated and encouraged employees to provide prompt and accurate information related to this event. No misoperations, system operating limits, or interconnection reliability operating limits were encountered during the course of this potential noncompliance.

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.)

This item was submitted by [REDACTED] on 1/5/2018

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: CIP-006-6
Applicable Requirement: R2.
Applicable Sub Requirement(s): 2.2.
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: Yes

If yes, indicate which Region(s):

Date Reported to Region(s):

9/2/2016

Date Possible Violation was discovered: 10/23/2017

Beginning Date of Possible Violation: 10/21/2017

End or Expected End Date of Possible Violation: 10/21/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

A contractor with unescorted NERC-CIP Physical Security Perimeter (PSP) access at [REDACTED] was escorting a visitor (contractor of the same company) inside the [REDACTED] for commissioning activities as part of the [REDACTED] Project on 10/21/2017. The escort properly logged the visitor into the [REDACTED] at 08:42, but neglected to log the visitor out of the [REDACTED] at the end of the day when they left site.

The escort properly logged the visitor into the manual logbook two days prior ([REDACTED] was not functioning at that time). In addition, the escort also properly logged the visitor into and out of the [REDACTED] the day prior. On 10/21/17, however the escort assumed that by selecting the duration of the visitor's stay in the [REDACTED] the system would automatically reject the visitor after the allotted time. Neither escort nor visitor were requested to complete training on the [REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Add [REDACTED] Training for anyone with PSP access to [REDACTED]

Install camera systems outside of the PSP's as a secondary means of control to help mitigate and identify all personnel that are entering and exiting the PSP.

Update [REDACTED] Training to include location of instructions on how to use the [REDACTED] and state instructions are available.

Update instructions posted above [REDACTED] and make the instructions more visible to the user.

Develop and implement a NERC Change Management Risk Assessment process / flow chart to help identify and get site management sign off of NERC process / procedure changes prior to implementation include timing of implementation / changes.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide details to prevent recurrence:

Update [REDACTED] Training to include location of instructions on how to use the [REDACTED] and to state instructions are available.

Update instructions posted above [REDACTED] and make the instructions more visible to the user.

Add [REDACTED] Training for anyone with PSP access to [REDACTED]

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

11/22/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power Electric System is categorized as moderate because if the personnel in PSP had caused harm, the electronic log would show the time they entered the space; only exit was not logged. The contractor had performed all training required to access the PSP. The visitor was observed during the entire duration of work within the PSP. Although the Contractor Escort and Visitor did not sign out of the [REDACTED] the Contractor Escort and Visitor did sign in and out of the [REDACTED] sign in log. Therefore, there is a record that the Contractor Escort and Visitor did leave the [REDACTED] PSP and site after their work shift was completed for the day.

Provide detailed description of Actual Risk to Bulk Power System:

There was no impact to the BES. The contractor had performed all necessary training and PRA requirements required to gain access to the PSP. The visitor was observed during the entire duration of work within the PSP. Although the Contractor Escort and Visitor did not sign out of the [REDACTED] the Contractor Escort and Visitor did sign in and out of the [REDACTED] Desk sign in log. Therefore, there is a record that the Contractor Escort and Visitor did leave the [REDACTED] PSP and site after their work shift was completed for the day.

Additional Comments:

N/A

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.)

Attachment 22

Record documents for the violation of CIP-006-3c R4

22.a The Companies' Self-Report 

This item was submitted by [REDACTED] on 6/16/2015

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: CIP-006-3c

Applicable Requirement: R4.

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): [REDACTED]

Date Reported to Region or Discovered by Region: 5/23/2013

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: 3/31/2015

Beginning Date of Possible Violation: 3/31/2015

End or Expected End Date of Possible Violation: 6/30/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-006-3c R4, [REDACTED] is obligated to document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) 24 hours a day, seven days a week.

On 3/31/15 [REDACTED] Specialist entered the [REDACTED] without NERC Access Authorization. At approximately 0815, the [REDACTED] Specialist contacted the [REDACTED] and advised he would only be walking around the outside performing a fire protection fire plan.

At 0840, the [REDACTED] received an Unauthorized Access Attempt from the [REDACTED] Specialist followed by a Door Forced Open Alarm at [REDACTED]

At 0841, the [REDACTED] contacted the [REDACTED] Specialist to advise him he does not have access to be inside the [REDACTED] and that he had triggered the alarm. [REDACTED] advised the [REDACTED] Specialist to return the key to Operations and do not swipe his badge in the area until access is granted and has been contacted by [REDACTED]

[REDACTED] immediately contacted the site Point of Contact (POC) and advised him of the [REDACTED] Specialist having a key to the [REDACTED] without having appropriate Access. The POC advised the [REDACTED] he would contact Operations to advise them that no one should be given the [REDACTED] if they do not have NERC Access clearance on their badge. This key was intended for use during emergency conditions only by authorized individuals to enter in case of the badge reader being down, medical, or fire emergencies.

The event occurred due to human performance issues with insufficient emergency [REDACTED] key control for the site, inadequate understanding of the badge reader controls, and inadequate means to verify NERC Access qualifications.

This violation is a [REDACTED] violation.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

[REDACTED]

Provide details to prevent recurrence:

[REDACTED]

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

6/30/2015

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:

The Potential Impact to the Bulk Power System is minimal because the [REDACTED] Specialist that entered the [REDACTED] was not NERC Access Authorized; however, he posed no risk to the equipment or function of the [REDACTED]. The [REDACTED] Specialist is [REDACTED] Badged and qualified for rounds and work within [REDACTED] and posed no threat or impact to the Bulk Electric System.

The unauthorized access alarm functioned properly to alert [REDACTED] which immediately contacted the [REDACTED] and the POC at the site, [REDACTED].

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this violation.

Additional Comments:

This violation was not the result of any intentional action by any involved party to violate any NERC reliability standard. Additionally, there were no misoperations, system operating limits, or interconnection reliability operating limits during the course of the noncompliance.

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.)

Attachment 23

Record documents for the violation of CIP-006-3c R5

23.a The Companies' Self-Report [REDACTED]

23.b The Companies' Self-Report [REDACTED]

23.c The Companies' Self-Report [REDACTED]

23.d The Companies' Self-Report [REDACTED]

23.e The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 7/14/2015

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: CIP-006-3c

Applicable Requirement: R5.

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): [REDACTED]

Date Reported to Region or Discovered by Region: 9/19/2014

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: 4/8/2015

Beginning Date of Possible Violation: 4/7/2015

End or Expected End Date of Possible Violation: 4/8/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-006-3c R5, [REDACTED] shall monitor physical access based on their documented and implemented technical and procedural controls for monitoring physical access.

On April 8, 2015, [REDACTED] failed to respond immediately to an unauthorized access attempt. The [REDACTED] performed a review of the Daily NERC Alarms and NERC Invalid Access Attempts reports. The report showed a total of seven alarms received on April 7, 2015 at the [REDACTED]. The report reflected a person attempting to enter the [REDACTED] who was not authorized for access to the Physical Security Perimeter (PSP).

[REDACTED] Unauthorized Badge Attempts for NERC Areas states that notification of the site contact(s) must be made if [REDACTED] receives five (5) or more unauthorized access attempts within five minutes. The report did not reflect information about contacting the site contact after receiving the five unauthorized access attempts. [REDACTED] notified [REDACTED] of the possible violation.

[REDACTED] investigated this incident on April 8, 2015 and discovered that a person exceeded five unauthorized badge attempts within five minutes. Seven (7) unauthorized badge attempts were executed on April 7, 2015 between 11:49:07am and 11:49:53am. A review of the records within the PACS did not reflect the correct response by the [REDACTED].

The incident was further reviewed with the [REDACTED] console operator and shift supervisor involved. Neither individual noticed the increase in alarm counts on the monitors during this time. Because of this, the [REDACTED] Unauthorized Badge Attempts for NERC Areas was not followed.

On April 20, 2015, [REDACTED] performed a series of multiple tests at the [REDACTED] to determine if there was an issue with the PACS or door hardware. Test results indicated

the PACS and door hardware was functioning as designed and no anomalies were reported.

On April 7, 2015, the console operator and shift supervisor were training several new security officers when this incident occurred.

At the time of this possible violation, the [REDACTED] contained a total of [REDACTED]

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

On April 15, 2015 and April 20, 2015 [REDACTED] conducted testing on multiple card readers to ensure that the Physical Access Control Systems (PACS) was functioning correctly and that the [REDACTED] was receiving the alarms accurately and in a timely manner.

[REDACTED] sent an e-mail to console operators and shift supervisors to reinforce the procedure for monitoring unauthorized access attempts.

Provide details to prevent recurrence:

The [REDACTED] Manager has conducted a coaching session with the Security Officers involved in the incident to reiterate the importance of carrying out the [REDACTED] Unauthorized Badge Attempts for NERC Areas procedure correctly.

[REDACTED] Unauthorized Badge Attempts for NERC Areas procedure will be reviewed and updated to provide clarity with alarm response. [REDACTED] console operators and shift supervisors will review the procedure and provide a formal acknowledgement.

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

10/31/2015

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:

The potential impact to the Bulk Power System is minimal because the [REDACTED] site continued to be secured and monitored on a 24 hour, 7 days per week basis.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this possible violation situation.

A report has been pulled to show all instances of 5 or more unauthorized badge attempts within 5 minutes from January 1, 2015 to June 5, 2015. Based on our review of this report, this incident of an inappropriate response only occurred on 4/7/2015 at the [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.)

This item was submitted by [REDACTED] on 3/1/2016

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: CIP-006-3c

Applicable Requirement: R5.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

7/14/2015

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: 12/29/2015

Beginning Date of Possible Violation: 12/16/2015

End or Expected End Date of Possible Violation: 1/2/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applied to [REDACTED]

On 11/14/2015 three new [REDACTED] were being converted from an old style [REDACTED] system to a new [REDACTED] system. The system was tested after the conversion and all functionality was tested, including the Loss of Communications even though it was not part of the checklist. The [REDACTED]

The [REDACTED] tested their NERC-CIP door alarms. Two of the NERC-CIP doors are wired to [REDACTED]. Both of these doors are monitored as exit only doors and will alarm the Command Center as soon as they are opened.

On 12/29/2015 when [REDACTED] tested the two doors (Door 4 and Door 5), the command center didn't receive the indication that the doors were opened, so the alarms were not received. The testing was part of a self assessment.

[REDACTED] created a Emergency Work Order for the [REDACTED] to come to site and test the functionality of the doors and alarms on 31 December 2015. The [REDACTED] was operational on January 2, 2016.

[REDACTED]

The [redacted] team came to the [redacted] and again tested all the Loss of Communications on all [redacted] at the site. The two year maintenance checklist is due to be completed prior to September 2016.

[redacted] has the same potential of locking up and not indicating a Loss of Communications. It is in the process of being tested.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The [redacted] team came to the [redacted] and tested all the Loss of Communications on all [redacted] at the site after the [redacted] was reset. The Loss of Communications functioned properly. Also, a line item to test loss of communications was added to the checklist.

Provide details to prevent recurrence:

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

9/30/2016

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:

The potential impact to the Bulk Power System was minimal because these are exit only doors and to open them the person needs to be inside the PSP. This means the person was either authorized to be inside or the escort with continuous visual monitoring of a person inside the PSP.

Provide detailed description of Actual Risk to Bulk Power System:

The actual Impact to the Bulk Power System is minimal because no systems were misoperated as a result of the doors 4 and 5 not being monitored.

Additional Comments:

This alleged violation was not a result of intentional action to violate a NERC reliability standard.

[redacted] was attempting to comply in good faith with the applicable NERC reliability standard at the issue in this instant alleged violation situation.

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.)

This item was submitted by [REDACTED] on 4/19/2016

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: CIP-006-3c

Applicable Requirement: R5.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

3/1/2016

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: 2/18/2016

Beginning Date of Possible Violation: 2/15/2016

End or Expected End Date of Possible Violation: 2/18/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-006-3 R5, Monitoring Physical Access, [REDACTED] shall document and implement the technical and procedural controls for monitoring physical access at all access points to the physical security perimeters.

On February 15 at 8:56 am an [REDACTED] operator received a [REDACTED] tamper alarm that came in on a [REDACTED]. The alarm should have been reset by the Supervisor.

An [REDACTED] noticed the alarm was in bypass mode on February 18 at 1:47 pm and armed it.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

1. The Officer (with Supervisor permissions) who put the alarm in bypass had her supervisor permissions removed and her Console Operator permissions.
2. We removed the ability for [REDACTED] Console operators to be able to bypass or reset alarms.
3. All [REDACTED] staff were retrained.

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include the following:

1. Console operators' permissions to bypass and reset alarms were removed.
2. All [REDACTED] staff were retrained.

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

2/22/2016

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is moderate because permissions ([REDACTED] Console Operators) were removed to bypass alarms immediately following occurrence or discovery of the incident.

Provide detailed description of Actual Risk to Bulk Power System:

The actual impact to the bulk power system as a result of this possible violation is minimal because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

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.)

This item was submitted by [REDACTED] on 8/11/2016

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: CIP-006-3c

Applicable Requirement: R5.

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: 6/28/2016

Beginning Date of Possible Violation: 6/28/2016

End or Expected End Date of Possible Violation: 6/29/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED] Per CIP-006-3c R5, [REDACTED] is obligated to document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty four hours a day, seven days a week.

During the Maintenance & Testing (M&T) inspection at the [REDACTED] on June 28, 2016 at 09:00, it was discovered that [REDACTED] & [REDACTED] on [REDACTED] wouldn't alarm when opened.

The Business Area entered a ticket for the security vendor to investigate and troubleshoot.

This is a 24/7 manned site. Roving Patrols were initiated for alternative measures during the period of troubleshooting and repair until this could be corrected. Alternative Measures started 6/28/2016 at 15:15 and ended 6/29/2016 at 15:00.

On Wednesday June 29, 2016, the security vendor arrived and reset the [REDACTED]. The doors still didn't alarm when opened. We contacted the [REDACTED] to let them know that the doors still didn't alarm correctly after the [REDACTED] reset. The [REDACTED] contacted the security vendor representative and they investigated the problem together.

The security vendor disconnected the wires and attached a meter to the ends at the [REDACTED]. He opened and closed the doors. The meter indicated continuity of the contacts. This means the wiring was good from the doors to the [REDACTED].

[REDACTED]

[REDACTED] changed the programming to supervised and then downloaded the [REDACTED]. The doors were retested again and alarmed correctly.

[REDACTED] discovered the issue through a Self-Assessment at the [REDACTED] while performing the two year M&T inspection.

Document BES Cyber System Information [REDACTED]

Document alternative measure forms [REDACTED] shows the Alternative Measures Activity log

Document [REDACTED] alarms functioning properly 6/29/2016 after [REDACTED] (Team) made the configuration supervision change.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Document [REDACTED] show that the [REDACTED] alarmed correctly on 6/29/2016 at 15:42.



Are Mitigating Activities in progress or completed?

If Yes, Provide description of Mitigating Activities:

[REDACTED] changed the programming for the supervision of doors 4&5 in the software configuration on June 29, 2016, so software and hardware installation would be consistent.



Provide details to prevent recurrence:

[REDACTED] is performing an investigation into the wiring versus programming for monitoring points as part of the investigation for an Apparent Cause Analysis (ACA). Corrective actions will be determined as an outcome of this investigation.



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

6/29/2016

Potential Impact to the Bulk Power System:

Actual Impact to the Bulk Power System:

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal because these are exit only doors and to open them the person needs to be inside the PSP. This means the person was either authorized to be inside or the escort with continuous visual monitoring of a person inside the PSP.

Provide detailed description of Actual Risk to Bulk Power System:

The actual Impact to the Bulk Power System is minimal because no systems were misoperated as a result of the doors 4 and 5 not being monitored

Additional Comments:

This alleged violation was not a result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at the issue in this instant alleged violation situation.

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.)

This item was submitted by [REDACTED] on 8/11/2016

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: CIP-006-3c
Applicable Requirement: R5
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):

Date Reported to Region or Discovered by Region:

4/19/2016

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: 4/14/2016

Beginning Date of Possible Violation: 4/14/2016

End or Expected End Date of Possible Violation: 12/30/2016

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]
Per CIP-006-3c R5, [REDACTED] is obligated to review unauthorized access attempts immediately and handle them in accordance with the procedures specified in Requirement CIP-008.

On April 14, 2016 the [REDACTED] notified the [REDACTED] that he believed there was a latency issue between the Physical Access Control System [REDACTED] and the operator interface software [REDACTED] causing a delay in notification from the alarm system to the security console operator for NERC and non-NERC alarms. The [REDACTED] was advised these delays were believed to exceed immediate review and handling relating to CIP-006-3c R5.

On April 15, 2016 a [REDACTED] requested the previous (30) days of NERC alarm history from a support person in the [REDACTED]. This alarm history was required to satisfy evidence requirements for CIP-006-3c.

On April 18, 2016 the support person provided the NERC alarms for all regions between 3/15/2016 and 4/15/2016. That individual explained that due to system limitations, he could not generate a report that ties [REDACTED] alarms back to the originating alarm in [REDACTED] so both interface alarm histories were provided separately. Upon analysis of the data, [REDACTED] delay could be attributed to system latency, system error, or operator error.

To determine if any of the [REDACTED] instances were acknowledged in either [REDACTED] requires an in-depth analysis of data. The format of the data currently

produced by the [REDACTED] is not sufficient as evidence to prove monitoring of NERC Physical Security Perimeters. At this time, it is suspected but not proven that there is and has been latency issues between [REDACTED] which are causing delays in NERC alarms being acknowledge by security console operators immediately. At this time, without a common tie (such as a transaction ID number, common name [REDACTED] number, etc.) [REDACTED] there is no way to sort data efficiently from the beginning of an alarm to its conclusion and no way to validate that alarms are being received [REDACTED] to know when or where to dispatch guards in response.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION



Are Mitigating Activities in progress or completed? 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:

The Potential Impact to the Bulk Power System is moderate because unauthorized access to BES Cyber Systems may occur and alarms may not be received by the security console operators within the 15 minute time period allowed. This could give an individual with malicious intent more time than NERC CIP standards prescribe as acceptable to negatively impact the Bulk Power System.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

Further discovery in the cause of this issue will be performed to determine a proper course of action and the cause of the latency. Due to some system limitations, this discovery is more difficult than expected. A lack of common identifier between systems has added complication to performing research.

[REDACTED] management has been involved in the process of discovering and reporting this issue.

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.)

Attachment 24

Record documents for the violation of CIP-007-3a R1.1

24.a Audit Summary [REDACTED]

24.b The Companies' Self-Report [REDACTED]

24.c The Companies' Self-Report [REDACTED]

24.d The Companies' Self-Report [REDACTED]

24.e The Companies' Self-Report [REDACTED]

[REDACTED]

Possible Violation (PV) / Find, Fix, and Track (“FFT”) Identification Form

This document is to be completed upon identification of a possible violation (PV), typically within 5 business days of the audit exit brief and emailed to [REDACTED] with a copy to [REDACTED]

For non-FFT candidates: Upon receipt of this document, Enforcement will coordinate with the reporting auditor and Enforcement to initiate the Enforcement processing of this possible violation.

Violation Reported By: [REDACTED]

Submittal Date: [Click here to enter text.](#)

Candidate for FFT Treatment: YES NO

Registered Entity: [REDACTED]

NERC Registry ID#: [REDACTED]

Compliance Monitoring Process: Compliance Audits

Standard, Version and Requirement in Violation: CIP-007-3a R1

Registered Function(s) in Violation: [REDACTED]

Initial PV Date (Actual Date Discovered by [REDACTED]

Date for Determination of Penalty/Sanction (Beginning Date of Violation): 9/03/2015

End Date of Possible Violation: Unknown

For Non-FFT Candidate ONLY

Violation Risk Factor: VRF - Medium

Violation Severity Level: Severe VSL

[REDACTED]

Potential Impact to Bulk Electrical System (BES): Minimal

Provide Explanation for Selection:

[REDACTED] did not follow their established change control process. Also [REDACTED] did not follow their implemented cyber security test procedures and did not document test results.

For Non-FFT and FFT Candidates

Basis for the PV:

Several instances of non-compliance were identified where the established change control process was not followed, required cyber security test procedures were not followed and test results were not documented. These instances would be violations of CIP-007-3 R1 (R1,R1.3) and CIP-003-3 R6.

Facts and Evidence pertaining to the PV:

Evidence:

- RSAW CIP-010-2_2015_v1_FINAL.pdf
- RFI-2-032.docx
- RFI-2-041.docx

Facts:

The audit team reviewed the RSAW narrative (*RSAW CIP-010-2_2015_v1_FINAL.pdf*) provided by [REDACTED] where they made the following statements:

“It was discovered that documentation of the test results, including the differences in the test environment, were not performed. For an example in which the business area has implemented the V5 compliance program, see “Change to Baseline.xlsx” for evidence of testing plan and procedures performed for a change, as well as documentation of verification of results.”
(*RSAW CIP-010-2_2015_v1_FINAL.pdf*, page 16)

The audit team issued RFI-2-032 requesting [REDACTED] to provide further details regarding the discovery that documentation of the test results, including the differences in the test environment, were not performed. [REDACTED] responded that “[...] documentation, as it relates to CIP-010 R1.5.2, was not sufficient to evidence testing of successful test results nor were description of measures used to account for differences between test and production.” (*RFI-2-032.docx*)

The audit team issued RFI-2-041 requesting examples of documentation that were not sufficient evidence of testing of successful test results. [REDACTED] responded with three examples of changes where sufficient evidence of testing and successful test results were not documented. The dates of those changes were 09/03/2015, 10/24/2015 and 10/28/2015. The narrative from *RFI-2-041.docx* for each is as follows:

1. On September 3, 2015, while working a "new install" ticket (46528) for asset [REDACTED] [REDACTED] the SME also installed [REDACTED] on the supporting server asset [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] however, the proper change control form was not submitted to support the installation of the software on the server.

On the morning on September 4, 2015 while reviewing a [REDACTED] SME realized that a change had taken place on asset [REDACTED] and that proper change control had not been followed. The [REDACTED] is an automated process that runs 1 time per day and compares the previous day's baselines with the current baselines to determine if there have been any changes. When the anomaly was identified [REDACTED] technician verified the software had been installed without following proper change control prior to installing the new software.

2. On October 24, 2015 [REDACTED] identified several changes to the baseline on asset [REDACTED]. An upgrade had been performed on October 23, 2015 to install [REDACTED] for [REDACTED] upgrade [REDACTED].
3. On October 28, 2015 [REDACTED] identified several changes to the baseline on asset [REDACTED]. An upgrade had been performed on October 27, 2015 to install [REDACTED].

The audit team finds a possible violation for CIP-007-3 R1 (R1,R1.3) and CIP-003-3 R6 due to not following the established change control process, not following required cyber security test procedures and not documenting test results.. The first issue reported occurred on September 3, 2015. Note that the audit is for CIP-010-1 R1 (Part 1.5) as part of the CIP Version 5 Transition Program.

For FFT Candidates ONLY

1. Why did this possible violation pose a minimal risk:
[Click here to enter text.](#)
2. Has Registered Entity mitigated this possible violation: YES NO
 - a. If yes, describe mitigating actions and state the date that Registered Entity completed the mitigating actions:

[Click here to enter text.](#)

[REDACTED]

3. Please answer the following questions to determine whether this possible violation constitutes a “clear on its face” FFT candidate or a “close call.” If the answer to any of the following questions is yes, this possible violation will be treated as a “close call.” Otherwise, this possible violation will be treated as a “clear on its face” FFT candidate.

A. Is there any disagreement amongst the audit team on whether the PV is a “clear on its face” or “close call” candidate: YES NO

a. If yes, explain why:

[Click here to enter text.](#)

B. Does this possible violation reveal a serious shortcoming in registered entity’s reliability-related processes (e.g. a systematic compliance program failure):

YES NO

a. If yes, explain why:

[Click here to enter text.](#)

C. Are there any additional facts the audit team needs to know in order to comfortably designate this possible violation for FFT treatment: YES NO

a. If yes, state those facts:

[Click here to enter text.](#)

4. Did audit team inform registered entity that this possible violation qualifies for FFT treatment? YES NO

a. If so, on what date? [Enter Date.](#)

This item was submitted by [REDACTED] on 8/4/2016

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: CIP-007-3a

Applicable Requirement: R1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

12/20/2012

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: 6/1/2016

Beginning Date of Possible Violation: 3/25/2016

End or Expected End Date of Possible Violation: 6/22/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]

Per CIP007-3a R1, [REDACTED] is obligated to ensure that new Cyber Assets and significant changes to existing cyber assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls.

R1.1 The Responsibility shall create, implement and maintain cyber security test procedures in a manner that minimized adverse effects on the production system or its operations.

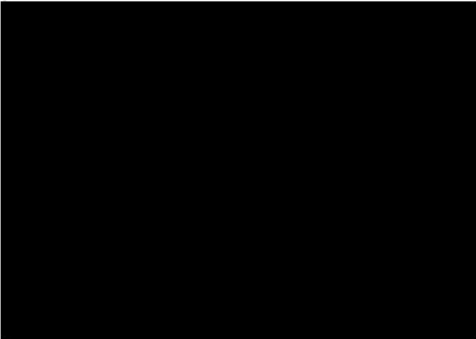
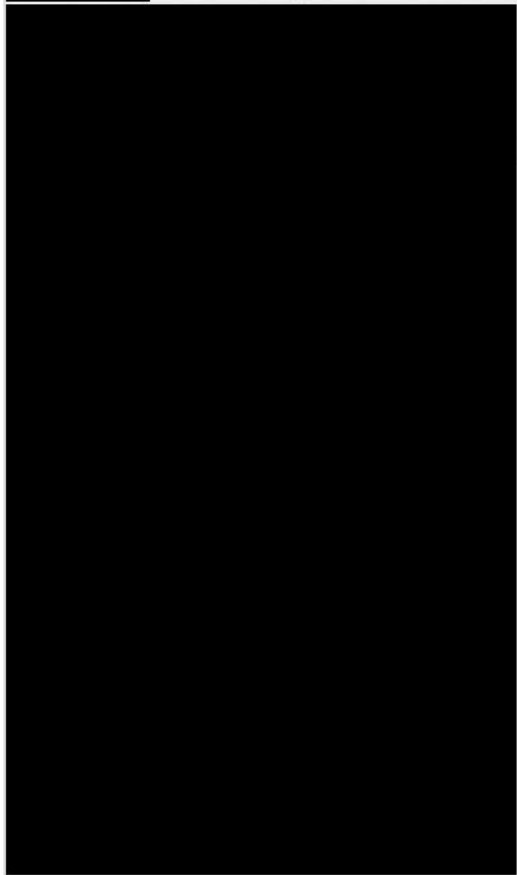
R1.2 The Responsibility shall document that testing is performed in a manner that reflects the production environment

R1.3 The Responsibility shall document test results.

On March 14, 2016 a [REDACTED] SME entered change request ticket 66046 in the [REDACTED] to install [REDACTED] on the identified list of assets. [REDACTED]

On June 1, 2016, while performing a review of other NERC CIP assets a [REDACTED] SME determined that the original change ticket (66046) was submitted to support the installation of [REDACTED] on the identified devices, however, that the status of the ticket was manually updated to 'Work in Progress' and therefore breaking the mechanics of the Change Control workflow in [REDACTED] which prevented testing to be completed on the NERC CIP assets.

On June 24, 2016 a new service desk ticket (68394) was entered into [REDACTED] to perform the appropriate testing on all NERC CIP assets identified on the original ticket.



Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:
Security Controls ticket 68394 was submitted on 6/10/2016 to perform testing on the NERC CIP assets originally identified on security controls ticket 66046.
On 6/22/2016 testing was completed on the identified NERC CIP assets.
Additionally, a Root Cause Analysis (RCA) is underway that will drive out other mitigating activities that should prevent a reoccurrence.

Provide details to prevent recurrence:

A Root Cause Analysis has also been performed. Future mitigation activities being considered to prevent recurrence include:
Implement the following changes/updates to [REDACTED]
1. Add checkbox ("Initiate Change") in [REDACTED] to indicate that all updates have been made to ticket and escalation can be run.
2. Lock asset tab to prevent additions following approval escalation.
Develop updated application and asset deployment Job Aid and/or guidance providing detailed instructions for proper execution of [REDACTED] change control activities when working with separate functional groups through:
1. Adoption of Job Aids and/or guidance specific to:
a. Data collection efforts (i.e. mapping data between CRQ and [REDACTED])
b. Aligning with [REDACTED] change control requirements. Ensure that all change control triggers are identified and captured.
c. Providing similar rigor as referenced in [REDACTED] including Risk Levels, Roles and Responsibilities, Human Performance tools, and consistent templates
d. Ensuring personnel do not exceed scope of change ticket per [REDACTED]
2. Development of method of conducting work that enforces operational discipline to execute a procedure (i.e. "Circle Slash" procedure, other HP Techniques, etc.).

Provide overview training for:

- 1. Updates to [REDACTED] functionality.
- 2. Application and asset deployment JobAid and/or guidance.

Enable [REDACTED] to manage volume of work through the following organizational considerations:

- 1. Allow [REDACTED] to engage with project managers in prioritization of work efforts.
- 2. Grant [REDACTED] ability to control schedule of work as a part of IT projects.

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

12/31/2016

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

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:

The Potential Impact to the Bulk Power System is minimal because physical access to the identified devices is limited to NERC CIP trained and authorized personnel. All devices that have syslog capability are monitored actively by a Security Event and Incident Management (SEIM) appliance [REDACTED]

Additionally, once the incident was discovered, mitigating steps were taken to implement change control process via a change control ticket that executed the appropriate security controls testing (Security Controls ticket 68394).

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

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.)

This item was submitted by [REDACTED] on 9/2/2016

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: CIP-007-3a

Applicable Requirement: R1.

Applicable Sub Requirement(s): R1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

6/30/2016

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: 5/17/2016

Beginning Date of Possible Violation: 5/16/2016

End or Expected End Date of Possible Violation: 5/18/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Applies to [REDACTED]
 On April 18th, 2016 at 8:00 AM, a change management ticket #66975 was entered into [REDACTED] (work management system) to upgrade the operating system on an [REDACTED] logging system (an Electronic Access Control and Monitoring device) from [REDACTED]. This work was intended to support the implementation of [REDACTED]. The [REDACTED] logging system was not appropriately associated to the change management ticket as a NERC CIP device by the SME who submitted the ticket.

[REDACTED] (a tool [REDACTED] uses to monitor system configuration changes) detected the configuration change performed in the change management ticket on May 17th, 2016. The change was detected a day after the upgrade was completed (on May 16th, 2016). Upon investigation, it was determined that the EACMS was not appropriately associated to the [REDACTED] ticket as a NERC CIP cyber asset. Because of this, the appropriate change management workflow and testing were not initiated.

The subject matter expert who submitted the first ticket also submitted a new change management ticket (#66731) on the afternoon of May 17th, 2016 and appropriately associated the EACMS to the ticket in order to rectify the error. This new ticket allowed the appropriate change and configuration management activities to occur on May 18th, 2016.

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Mitigation was completed on May 18, 2016. On May 17, 2016, the SME submitted a new change management ticket (#66731) and appropriately associated the EACMS to the ticket as NERC CIP Cyber Asset. This allowed the required workflows to occur as required. Those workflows prompt for required activities such as testing of configuration changes. A cause analysis will be performed to determine what future corrective actions are required.

Provide details to prevent recurrence:

A cause analysis will be performed to determine the best course of action to ensure this issue does not occur again.

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

5/26/2016

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:

The potential impact to the Bulk Electric System would be that a change could be made to a NERC CIP EACMS that was not expected or desired during the update process. This could allow for a security risk to exist that may have been discovered and mitigated if the correct change control process was followed. Compromise would be unlikely or risk would have been limited due to the other protections provided via the NERC CIP requirements and the protections placed upon EACMs. Those protections would keep the impact to a minimal possibility.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation. No security issues are known to have resulted from this change and no negative impacts to the Bulk Power System have been discovered. [REDACTED] captured and alerted support to the change on May 16th, 2016. A new ticket was created May 17th, 2016 which properly associated the EACMS to the ticket as a NERC CIP cyber asset. With the Cyber Asset properly associated, the appropriate workflow was performed and the actions required to meet compliance were completed.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

The individual who submitted the initial change ticket did not answer some questions correctly.

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.)

This item was submitted by [REDACTED] on 9/2/2016

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: CIP-007-3a

Applicable Requirement: R1.

Applicable Sub Requirement(s): R1.3.

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: 8/10/2016

Beginning Date of Possible Violation: 4/30/2015

End or Expected End Date of Possible Violation: 8/31/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]

1. [REDACTED] On 7/22/2015; [REDACTED] Employees were at [REDACTED] performing the Patch Management Program for NERC CIP. During that project, the [REDACTED] was replaced because it was part of the Patch Management Program. At that time, an [REDACTED] failed and needed to be replaced. These changes were conducted without updating our system of record [REDACTED]. Also, communication did not take place to advise engineering of the changes so the baselines could be updated and a security controls testing performed.

During the annual CIP Walkdown on 08/10/2016; it was discovered that a [REDACTED] were replaced on 7/22/2015 without documenting these changes, updating the system security baseline and performing necessary security controls testing. The System of Record [REDACTED] has been updated with the correct information. An Extent Of Condition Analysis was conducted; IT and [REDACTED] have SRs for like requirements.

[REDACTED]

2. [REDACTED] During an annual CIP Walkdown at [REDACTED] on 08/10/2016; it was discovered that a firmware change was conducted on a [REDACTED] in May of 2015 without documenting the change, or performing necessary security controls testing. The System of Record [REDACTED] has been updated with the correct information. An Extent Of Condition Analysis was conducted; IT and [REDACTED] have SRs for like requirements.

[REDACTED]

3. [REDACTED] On 4/30/2015; [REDACTED] employees were at [REDACTED] performing work as part of [REDACTED]. During this project, a [REDACTED] was installed, but it was not documented in the system of record [REDACTED]. This was discovered during the annual CIP Walkdown on 08/11/2016. This [REDACTED] was installed on [REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

On 08/31/2016 the baseline and firmware strings were updated in [REDACTED]

We will ensure that these devices meet an existing filed baseline by providing documentation that shows they comply with an existing baseline using methods of collecting information and screenshots.

Provide details to prevent recurrence:

To prevent reoccurrence, additional Change Management Training will be conducted and the importance of keeping accurate [REDACTED] records will be re-communicated.

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

9/30/2016

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:

The Potential Impact to the Bulk Power System is minimal because the device is located within the PSP (Physical Security Perimeter, the assets were in the defined ESP (Electronic Security Perimeter), All routable devices were accessed through the EAP (Electronic Access Point), and these devices were monitored for security events.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation. [REDACTED] senior management and direct managers relevant to the situation actively participated and encouraged employees to provide complete information.

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.)

This item was submitted by [REDACTED] on 8/11/2017

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: CIP-007-3a

Applicable Requirement: R1.

Applicable Sub Requirement(s): R1.3.

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): [REDACTED]

Date Reported to Region or Discovered by Region: 9/5/2012

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: 6/14/2017

Beginning Date of Possible Violation: 5/9/2016

End or Expected End Date of Possible Violation: 6/15/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-007-3a, R1 the Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter (ESP) do not adversely affect existing cyber security control. For purposes of Standard CIP007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

Sub-requirement R1.3, requires the Responsible Entity to document test results.

On 6/14/2017, [REDACTED] was performing a CIP v5 Paper Vulnerability Assessment activity. During the validation and verification between the IT Asset Inventory [REDACTED] the [REDACTED] asset repository from [REDACTED] it was discovered that [REDACTED] was not scanned for security controls at the time of deployment on May 9, 2016, under CIP v3.

Based on system/logging information, it was determined that a clerical error occurred when the [REDACTED] was initially processed. This ticket was closed without the proper classification being set on the asset in question. [REDACTED] uses the assigned classification to automatically execute the appropriate NERC CIP BES Cyber Asset workflows to create the subsequent Security Controls Testing (SCT) tickets and proper BES Cyber Asset classification.

Although this asset was not commissioned through the normal [REDACTED] ticket flow processes, security tools and monitoring were implemented and performed as of July 3, 2016, per [REDACTED] the change management, monitoring and alerting tool used by [REDACTED]

On 6/14/2017 a [REDACTED] security controls ticket (SCT-2121) was created and security controls testing completed on 6/15/2017.

A cause analysis is being performed which will include a mitigation plan to remediate the causes of the potential violation.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Are Mitigating Activities in progress or completed? 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:

Using the CIP Violation Risk Factor version 3 table, the region has identified the potential risk to the Bulk Power System as "Lower" because the Responsible Entity did not document test results prior to installing this BES Cyber Asset on the ESP, per sub-requirement R1.3.

On 6/14/2017, the same day the issue was identified, immediate steps were taken to address the lack of a security controls test for this device. A [REDACTED] SCT was created and security controls testing completed on 6/15/2017 with no NERC CIP implications identified. In addition, the BES Cyber Asset in question is located within a Physical Secured Perimeter (PSP) and is on an ESP that is monitored 24x7x365. Only those individuals who are NERC CIP trained and have a valid Personnel Risk Assessment (PRA) are authorized to access this device.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there was no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of the possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

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.)

Attachment 25

Record documents for the violation of CIP-007-6 R1

25.a The Companies' Self-Report [REDACTED]

25.b The Companies' Self-Report [REDACTED]

25.c The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 8/31/2016

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: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.2.

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: 7/20/2016

End or Expected End Date of Possible Violation: 7/20/2016

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP-002-5.1 R1.2, [REDACTED] is obligated to identify and classify Medium Impact Electronic Access Control and Monitoring Systems (EACMS).

During a review of the asset list, it was discovered that a Security Event and Incident Monitoring (SEIM) device was not labeled as and EACMS as expected. As a result, the devices were not evaluated for application of [REDACTED] and NERC CIP controls. Upon investigation, the [REDACTED] discovered that during implementation, the process to identify EACMS was followed, however the process did not specify inclusion of devices outside of the Electronic Security Perimeter (ESP). Therefore during classification of the devices, the SEIM was not classified as EACMS at [REDACTED].

The classification took place during the implementation of [REDACTED] before the compliance date.

[REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

If Yes, Provide description of Mitigating Activities:

[Redacted] has reviewed the SEIM classification and is in the process of performing a walk down at each station to reapply the internal policy for classifying an EACMS

Provide details to prevent recurrence:

Actions to prevent recurrence will be developed as part of the mitigation plan.

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

11/18/2016

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:

Potential impact to the BPS is minimal because the device currently has several additional protections in place when compared to other non-CIP assets. [Redacted]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

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.)

This item was submitted by [REDACTED] on 4/7/2017

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: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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: 1/5/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 1/11/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

[REDACTED]

[REDACTED]

The devices [REDACTED] reside in the [REDACTED] and the following number of devices are with this BCS:

[REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Yes, these devices were reclassified as follows:

Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide details to prevent recurrence:

A cause analysis will be performed to evaluate additional causal factors to identify effective corrective actions to prevent reoccurrence.

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

1/11/2017

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:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

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.)

This item was submitted by [REDACTED] on 1/23/2018

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

4/7/2017

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: Yes

If yes, indicate which Region(s):

[REDACTED]

Date Reported to Region(s):

4/7/2017

Date Possible Violation was discovered: 11/15/2017

Beginning Date of Possible Violation: 11/15/2017

End or Expected End Date of Possible Violation: 11/17/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED] and [REDACTED]

Per CIP002-5, R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

Per sub-requirement R1.1:

Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

Problem Statement

[REDACTED] were not properly classified as High Impact Electronic Access Control or Monitoring Systems (EACMS), causing the devices to potentially not have full North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), resulting in this possible violation.

Additional Information:

Categorization of Bulk Electric System (BES) Cyber Assets (CAs), BCAs, is the process whereby a CA and then assigns the appropriate categorization to that device. Proper categorization of EACMS ensures appropriate NERC CIP protections are implemented on the identified asset.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

[Redacted]

Method of Discovery

Self-Assessment: [Redacted]

[Redacted]

Extent Of Condition:

As part of the [Redacted] the [Redacted] group will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all [Redacted] will need to 1) reassess their technologies to ensure alignment with the [Redacted] and 2) ensure [Redacted] Level processes support the new program which may require the [Redacted] to work through the asset classification process for all assets under the revised program.

Cause Analysis:

This violation occurred as a result of:

- Lack of specificity within the [Redacted] requirements of the process, no process available.

Cause Identification:

- Prior self-reported issues with [Redacted] and other firewall rules focused on systems designed to facilitate IRA were incorrectly implemented due to the lack of clarity in the [Redacted] program
- [Redacted] and [Redacted] were not properly assessed in the V5 transition as being Intermediate Systems
- [Redacted] and [Redacted] were not previously identified as EACMS because their primary function was not to enable remote access

The direct and contributing causes of this possible violation:

Apparent Cause 1 (AC1): Process Weakness. Lack of specificity within the [Redacted] requirements of the process; no process available.

Prior self-reported issues with [Redacted] and other firewall rules, focused on systems designed to facilitate IRA and were incorrectly implemented due to the lack of clarity during the implementation of the [Redacted] program.

[Redacted]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Actions [Redacted] has already completed to remediate this potential violation include:

On 11/28/2017, [Redacted] determined this violation a self-report and the [Redacted] team submitted the appropriate [Redacted] ticket workflow to correctly update the categorization and create the necessary work orders to apply the appropriate controls to the identified devices.

Completed: As of 12/4/2017, all identified devices have been re-categorized as EACMS.

Provide details to prevent recurrence:

██████████ has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that ██████████ will incur further risk of the same or similar NERC reliability standard violation.

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE. THIS INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

See section 7.0 Corrective Actions (Fixes) Recommended by Cause Analysis Team for respective milestone dates.

- CIP-002 ██████████ ██████████ ██████████ to provide updated CIP-002 ██████████ documentation that will be used by all ██████████ ██████████ to perform a gap analysis and re-evaluation of in-scope BES Cyber Assets
- With oversight from ██████████ all ██████████ to perform a business procedure / gap analysis between the current CIP-002 / ██████████ business procedures and the updated CIP-002 / ██████████ documentation
- With oversight from ██████████ all ██████████ to provide a draft of CIP-002 / ██████████ business level procedures
- With oversight from ██████████ all ██████████ to obtain ██████████ business level procedures approved
- With oversight from ██████████ all ██████████ to identify those individuals who require training on updated CIP-002 / ██████████ business level procedures
- With oversight from ██████████ all ██████████ to communicate and provide training on updated CIP-002 / ██████████ business level procedures to those individuals requiring training
- With oversight from ██████████ all ██████████ to re-evaluate / re-classify BES Cyber Assets based on updated business level procedures and submit potential violation if identified
- ██████████ to submit ██████████ tickets to initiate workflow necessary to re-classify identified devices as EACMS
- ██████████ to perform an active review of All ██████████ Management Systems to determine if any additional systems have been improperly classified
- ██████████ to submit ██████████ tickets to push firewall rules for scanning identified devices
- ██████████ to perform security controls testing (SCT) on identified devices

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

11/28/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

Baseline management including:

- 1) Operating system/firmware
- 2) Software version
- 3) Logical network accessible ports
- 4) Security patches
- 5) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

██████████ did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

The likelihood that this event would adversely impact the Bulk Electric System is considered minimal because:



Additional Comments:

This violation was not the result of intentional action to violate a NERC reliability standard. ██████████ was attempting to comply in good faith with the applicable NERC reliability standard at issue in this potential violation. The ██████████ internal compliance plan was in effect at the time of the potential noncompliance. ██████████ management relevant to the situation actively participated and encouraged employees to provide complete information.

There have been no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance.

Attachment 26

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

- 26.a The Companies' Self-Report [REDACTED]
- 26.b The Companies' Self-Report [REDACTED]
- 26.c The Companies' Self-Report [REDACTED]
- 26.d The Companies' Self-Report [REDACTED]
- 26.e The Companies' Self-Report [REDACTED]
- 26.f The Companies' Self-Report [REDACTED]
- 26.g The Companies' Self-Report [REDACTED]
- 26.h The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED]

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: CIP-007-6

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.2.

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: 8/3/2016

Beginning Date of Possible Violation: 8/3/2016

End or Expected End Date of Possible Violation: 8/30/2016

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED]

Per CIP-007-5

R 2.2 At least once every 35 calendar days evaluate security patches for applicability that have been released since the last evaluation from the source or sources;

R2.3 For applicable patches identified in part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:

Apply the patch or create a dated mitigation plan or revise an existing mitigation plan.

During audit preparation review sessions in [REDACTED] it was determined that [REDACTED] failed to monitor vendor security patches and vulnerability notifications at least once every 35 calendar days as required by CIP Version 5 for [REDACTED] that have the [REDACTED] application installed during the past 12 months as documented in [REDACTED]

The [REDACTED] team has a patch management process but does not currently include monitoring for [REDACTED] devices that have [REDACTED] application installed.

[REDACTED] The [REDACTED] shall identify sources for software patches and monitor for available system vendor security patches and vulnerability notifications when the devices are updateable and for which a patching source exists. If a vulnerability is reported during the monitoring process that is not addressed by a security patch, the [REDACTED] shall document it and send it to the [REDACTED] process for disposition.

An extent of condition was performed which identified the following [REDACTED] devices that have the [REDACTED] application installed:

[REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because

Electric System.

This application does not have direct access to the Bulk

Although there is a potential that a security vulnerability could be exploited, the likelihood of this considered minimal.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there was no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of the alleged violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

was attempting to comply in good faith with the applicable NERC reliability standard at issue in this possible violation situation.

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.)

This item was submitted by [REDACTED] on 8/14/2017

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: CIP-007-6

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.2.

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: 10/6/2016

Beginning Date of Possible Violation: 8/29/2016

End or Expected End Date of Possible Violation: 10/6/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP-007-5, R2.2, [REDACTED] is obligated to:

At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.

[REDACTED] did not develop a process for managing cyber security [REDACTED] software patch updates in accordance with Compliance Procedure [REDACTED]. As a result proper controls were not in place. Also, ownership and accountability was not clearly defined for the stakeholders. This became apparent when a failure to respond on time to a cyber security software patch pertaining to a [REDACTED] device was not completed within the specified time frame as required by CIP-007-5 R2.2. According to the NERC-CIP requirement, monitoring of new [REDACTED] security patches and the evaluation of these patches must both be completed within thirty-five (35) days of the date that the relay security patch was initiated by the vendor.

[REDACTED]

[REDACTED]

The actions that [REDACTED] is taking to prevent recurrence include the following:

- 1.) An interim measure was implemented to have

specify a completion due date and to provide the current tracking spreadsheet for all patch notification sent to [REDACTED]

Due Date: Complete 1/20/2017

REDACTED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

- 2.) Communicate the findings of this ACA for [REDACTED] cyber security software patches to Engineering groups in the other region. Due Date: Complete 1/20/2017
- 3.) Develop a process that would assist management with visibility of the [REDACTED] cyber security software patch program. Due Date: 10/31/17
- 4.) Document a comprehensive Compliance Department / Engineering Department security patch process for monitoring, evaluating, documenting, tracking and applying cyber security software patches for [REDACTED] assets for all regions of [REDACTED] Engineering that is consistent with the [REDACTED]. Due Date: 11/30/17
- 5.) Review documented process in action item #6 and validate that actions are owned by and notifications are made to at least 2 individuals in the Engineering Department. Due Date: 11/30/17
- 6.) [REDACTED] will perform a review to determine the effectiveness of the corrective actions described above. Due Date: 8/31/18

Are Mitigating Activities in progress or completed? No [REDACTED]

Potential Impact to the Bulk Power System: Minimal [REDACTED]

Actual Impact to the Bulk Power System: Minimal [REDACTED]

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because [REDACTED] once reviewed did not negatively impact the [REDACTED] devices currently in-service protecting the bulk electric system.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

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.)

This item was submitted by [REDACTED] on 9/5/2017

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: CIP-007-6

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.2.; 2.3.

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: 2/24/2017

Beginning Date of Possible Violation: 8/31/2016

End or Expected End Date of Possible Violation: 5/24/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Patch evaluations and subsequent Patch Mitigation Plans are required for Medium Impact BES Cyber Systems. While performing March 2017 security patch evaluations, it was discovered that [REDACTED] January 2017 patch evaluations and patch mitigation plans were not stored on the [REDACTED]. To correct the noncompliance, January 2017 evaluations were promptly performed. Further investigations revealed gaps in patch evaluation documentation quality. This is a possible violation for NERC CIP compliance.

NERC requirements also require the implementation of patches or a patch mitigation plan that outlines when the patch will be implemented. If the patch mitigation plan cannot be implemented in the specified timeline, an extension must be approved by the CIP Sr. Manager or delegate. [REDACTED] does not have a tracking mechanism in place for patch mitigation plans and [REDACTED] have existing patch mitigation plans that are past due.

The compliance team is responsible for performing the patch evaluations. There is no work ticketing tool in place for [REDACTED] CIP compliance tasks. Compliance team leadership is currently working with [REDACTED] to enter the tasks into [REDACTED] for tracking. The process does not currently contain enough detail for the compliance analyst to effectively perform the evaluation and store evidence appropriately. The compliance manager did not provide sufficient oversight to ensure evaluations were being completed and stored.

The [REDACTED] Extent of Condition investigation provided information that the security patch management program was deficient across all of [REDACTED] and [REDACTED] with multiple possible violations due to the patch management.

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Immediately, an evaluation and documentation per [REDACTED] was performed.

Provide details to prevent recurrence:

The following steps will be taken in order to prevent recurrence:

Ongoing Compliance Execution Tasks were added for Monthly Patching Activity via

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

Oversight Execution Tasks were added for Compliance Managers to complete Activity Oversight for monthly patching activities via

Task management and oversight will be included into the as part of

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

6/16/2017

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:

The Potential Impact to the Bulk Power System is minimal because this was a documentation error.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this potential violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this violation.

Additional Comments:

No 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.)

This item was submitted by [REDACTED] on 9/12/2017

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: CIP-007-6

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.2.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

8/10/2017

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: Yes

If yes, indicate which Region(s):

[REDACTED]

Date Reported to Region(s):

8/10/2017

Date Possible Violation was discovered: 5/1/2017

Beginning Date of Possible Violation: 9/14/2016

End or Expected End Date of Possible Violation: 10/15/2017


Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

In 2015, the [REDACTED] created a procedural document (Standard Operating Procedure for Security Patches, document number [REDACTED]) to manage Bulk Electric System (BES) cyber security assets (attached). This document describes the procedure for [REDACTED] security patch management program for BES cyber assets. [REDACTED] became aware of security patches for [REDACTED] (there were [REDACTED] security patches for these devices released from August 9th 2016 through April 6, 2017) when [REDACTED] notified them on April 28th, 2017 of a security patch release on April 6, 2017. This notification led [REDACTED] to review their security patch procedure and determined that [REDACTED] had not reviewed these patches within the 35 day window (CIP-007-6 R2.2) in the [REDACTED]. Due to the fact that that the security patch notification method (website) was changed without [REDACTED] knowledge, following the [REDACTED] would not have prevented the violation. The violation occurred on September 14, 2016 (day 36 following the first of [REDACTED] security patches for the [REDACTED] was released).

Are Mitigating Activities in progress or completed? Yes

 An Informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to make the Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Immediate Mitigating Activities:

1. Notification of [redacted] security patches sent to [redacted] for immediate review of the [redacted] security patches as required by CIP-007-6 R 1
2. [redacted] were discovered in [redacted] and added to the list of devices tracked for security patch management.
3. [redacted] reviewed security patches and determined that the security patches did not apply to the [redacted] in the [redacted]
4. Extent of Condition information collected from [redacted] and were completed on 8/16/2017.

Provide details to prevent recurrence:

[redacted] has taken or plans to take with respect to this issue include the following:

1. Notification of [redacted] security patches sent to [redacted] for immediate review of the five [redacted] security patches. (Complete)
2. [redacted] devices were discovered in [redacted] and added to the list of devices tracked for security patch management. (Complete)
3. [redacted] reviewed security patches and determined that the security patches did not apply to the [redacted] devices in the [redacted] (Complete)

Additional activities to be completed:

4. Develop a charter for a cross-jurisdictional [redacted] to oversee and monitor security patch management for [redacted] including process development and refinement and training.

5. Update Security Patch List

6. Assess the effectiveness of the existing [redacted] as a tracking tool and auditing document.

NOTE: This Corrective Action will be completed under Corrective Action #3, the [redacted] mitigation plan [redacted]

7. Regarding Corrective Action #6. If applicable, develop a new tool or modify the existing spreadsheet to more accurately identify and track security patches.

NOTE: This Corrective Action will be completed under Corrective Action #4, the [redacted] mitigation plan [redacted] and supports this ACA.

8. Document a comprehensive Compliance Department / Engineering Department security patch process for monitoring, evaluating, documenting, tracking and applying cyber security software patches for relay assets for all regions of [redacted] that is consistent with the [redacted]

NOTE: This Corrective Action will be completed under Corrective Action #6, the [redacted] mitigation plan [redacted] and supports this ACA.

9. Provide training to those stakeholders responsible for monitoring, evaluating, documenting and tracking cyber security software patches for relay assets. [redacted] needs to review evidence of completion of this corrective action two weeks prior to the due date.)

NOTE: This Corrective Action will be completed under Corrective Action #12, the [redacted] mitigation plan [redacted] and supports this ACA.

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

12/12/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Potential Impact – The Potential Impact to the Bulk Electric System is minimal because the [redacted] Devices that these security patches were released for are not accessible via Electronic Routable Connectivity (ERC) and are located inside a secure Physical Security Perimeter. In order to exploit the vulnerability, an adversary would need to defeat the physical security controls to gain direct access to the devices.

Provide detailed description of Actual Risk to Bulk Power System:

Actual Impact - The security patches were determined as not applicable to the devices. As a result, there was no actual impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

[Redacted area for 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.)

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

This item was submitted by [REDACTED]

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: CIP-007-6

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.3.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

9/6/2014

Monitoring Method for previously reported or discovered:

Self-Certification

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: 12/7/2016

Beginning Date of Possible Violation: 7/15/2016

End or Expected End Date of Possible Violation: 3/7/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

On December 7, 2016, while preparing for the [REDACTED] the [REDACTED] Subject Matter Expert (SME) responsible for [REDACTED] was reviewing the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. As a result of the review the SME identified and self-reported, he had previously misinterpreted the requirement to create a new or revise an existing patch mitigation plan within 35 days after completing a security patch evaluation.

Although the monitoring, analysis, and documentation of [REDACTED] security patches were being completed within the 35 day requirement as outlined in CIP-007-5 R2.2, a dated Patch Mitigation Plan describing security vulnerability remediation, and the timeframe for completion of mitigation steps was not created.

The missing mitigation plans are associated with [REDACTED] Cyber Assets identified as Cyber Assets associated with a Bulk Electric System (BES) Cyber System in the Asset Identification and Classification (AIC) list.

During review of the incident, the following potential causes were identified.

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Completed mitigation activities include the following:

1. Upon notification of a possible violation related to the creation of Patch Mitigation Plans, the [redacted] immediately assembled all [redacted] Subject Matter Experts to complete a review of requirements related to CIP-007-6 and [redacted]

(Date: 12/7/2016 day of possible violation discovery, Status: Completed)

2. Made current or developed new [redacted] to correspond with completed security vulnerability assessments.
- Updated one existing Patch Mitigation Plan to include additional scope.

4. Established a monthly QA procedure to ensure applicable security patches have been analyzed and applied, or Patch Mitigation Plans have been developed or revised within the 35 day requirement outlined in CIP-007-6 R2.3. At the conclusion of the monthly QA review, [redacted] confirms the Patch analysis and Mitigation Plan process is current by providing a dated signature within the Patch Management Review tracking sheet.

Provide details to prevent recurrence:

To prevent recurrence of the identified possible violation, the monthly QA procedure will be formally documented and approved by 5/1/2017.

A cause analysis will be performed to evaluate additional causal factors and to identify effective corrective actions to prevent reoccurrence.

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

1/6/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is moderate because of [redacted] implementation of layered security controls. These layered controls include 1) limited physical access to facilities, 2) all devices located within a defined Electronic Security Perimeter, which denies access from the outside by default, 3) Intrusion Prevention and Detection Systems to monitor traffic inbound and outbound of High Impact locations.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

In addition, even though Patch Mitigation Plans were either not revised or created within the requirement date outlined in CIP-007-6, published security vulnerabilities continued to be monitored and evaluated for risk to the enterprise.

Based on the [redacted] no high risk vulnerabilities were identified and only one medium risk vulnerability was identified during the timeframe of the possible violation.

Additional Comments:

[redacted] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this possible violation. In addition, this possible violation was not the result of intentional action to violate a NERC reliability standard.

This item was submitted by [REDACTED] on 8/31/2016

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: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.2.

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: 7/20/2016

End or Expected End Date of Possible Violation: 7/20/2016

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP-002-5.1 R1.2., [REDACTED] is obligated to identify and classify Medium Impact Electronic Access Control and Monitoring Systems (EACMS).

During a review of the asset list, it was discovered that a Security Event and Incident Monitoring (SEIM) device was not labeled as and EACMS as expected. As a result, the devices were not evaluated for application of [REDACTED] and NERC CIP controls.

Upon investigation, the [REDACTED] discovered that during implementation, the process to identify EACMS was followed, however the process did not specify inclusion of devices outside of the Electronic Security Perimeter (ESP). Therefore during classification of the devices, the SEIM was not classified as EACMS at [REDACTED]

The classification took place during the implementation of [REDACTED] before the compliance date.

[REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

If Yes, Provide description of Mitigating Activities:

[Redacted] has reviewed the SEIM classification and is in the process of performing a walk down [Redacted] to reapply the internal policy for classifying an EACMS

Provide details to prevent recurrence:

Actions to prevent recurrence will be developed as part of the mitigation plan.

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

11/18/2016

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:

[Redacted]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

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.)

This item was submitted by [REDACTED] on 4/7/2017

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: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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: 1/5/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 1/11/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:
Yes, these devices were reclassified as follows:

- a. [REDACTED] - 74357 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- b. [REDACTED] - 74363 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- c. [REDACTED] - 74355 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17

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

Provide details to prevent recurrence:

A cause analysis will be performed to evaluate additional causal factors to identify effective corrective actions to prevent reoccurrence.

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

1/11/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal [REDACTED]

Actual Impact to the Bulk Power System: Minimal [REDACTED]

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

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.)

This item was submitted by [REDACTED] on 1/23/2018

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

4/7/2017

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: Yes

If yes, indicate which Region(s):

[REDACTED]

Date Reported to Region(s):

4/7/2017

Date Possible Violation was discovered: 11/15/2017

Beginning Date of Possible Violation: 11/15/2017

End or Expected End Date of Possible Violation: 11/17/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP002-5, R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

Per sub-requirement R1.1:

Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

Problem Statement

[REDACTED] were not properly classified as High Impact Electronic Access Control or Monitoring Systems (EACMS), causing the devices to potentially not have full North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), resulting in this possible violation.

Additional Information:

Categorization of Bulk Electric System (BES) Cyber Assets (CAs), BCAs, is the process whereby a CA and then assigns the appropriate categorization to that device. Proper categorization of EACMS ensures appropriate NERC CIP protections are implemented on the identified asset. PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Method of Discovery

Self-Assessment: [REDACTED]

Extent Of Condition:

As part of the [REDACTED] the [REDACTED] group will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all [REDACTED] will need to 1) reassess their technologies to ensure alignment with [REDACTED] and 2) ensure [REDACTED] Level processes support the new program which may require the [REDACTED] to work through the asset classification process for all assets under the revised program.

Cause Analysis:

This violation occurred as a result of:

- Lack of specificity within the [REDACTED] requirements of the process, no process available.

Cause Identification:

- Prior self-reported issues with [REDACTED] focused on systems designed to facilitate IRA were incorrectly implemented due to the lack of clarity in [REDACTED]
- [REDACTED] were not properly assessed in the V5 transition as being Intermediate Systems
- [REDACTED] were not previously identified as EACMS because their primary function was not to enable remote access

The direct and contributing causes of this possible violation:

Apparent Cause 1 (AC1): Process Weakness. Lack of specificity within the [REDACTED] requirements of the process; no process available.

Prior self-reported issues with [REDACTED] focused on systems designed to facilitate IRA and were incorrectly implemented due to the lack of clarity during the implementation of the [REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

[An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.](#)

If Yes, Provide description of Mitigating Activities:

Actions [REDACTED] has already completed to remediate this potential violation include:

On 11/28/2017, [REDACTED] determined this violation a self-report and the [REDACTED] submitted the appropriate [REDACTED] ticket workflow to correctly update the categorization and create the necessary work orders to apply the appropriate controls to the identified devices.

Completed: As of 12/4/2017, all identified devices have been re-categorized as EACMS.

Provide details to prevent recurrence:

has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that will incur further risk of the same or similar NERC reliability standard violation.

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

See section 7.0 Corrective Actions (Fixes) Recommended by Cause Analysis Team for respective milestone dates.

- CIP-002 to provide updated CIP-002 documentation that will be used by all to perform a gap analysis and re-evaluation of in-scope BES Cyber Assets
- With oversight from all to perform a business procedure / gap analysis between the current CIP-002 / business procedures and the updated CIP-002 documentation
- With oversight from all to provide a draft of CIP-002 business level procedures
- With oversight from all to obtain business level procedures approved
- With oversight from all to identify those individuals who require training on updated CIP-002 / business level procedures
- With oversight from all to communicate and provide training on updated CIP-002 / business level procedures to those individuals requiring training
- With oversight from all to re-evaluate / re-classify BES Cyber Assets based on updated business level procedures and submit potential violation if identified
- to submit tickets to initiate workflow necessary to re-classify identified devices as EACMS
- to perform an active review of All Management Systems to determine if any additional systems have been improperly classified
- to submit tickets to push firewall rules for scanning identified devices
- to perform security controls testing (SCT) on identified devices

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

11/28/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

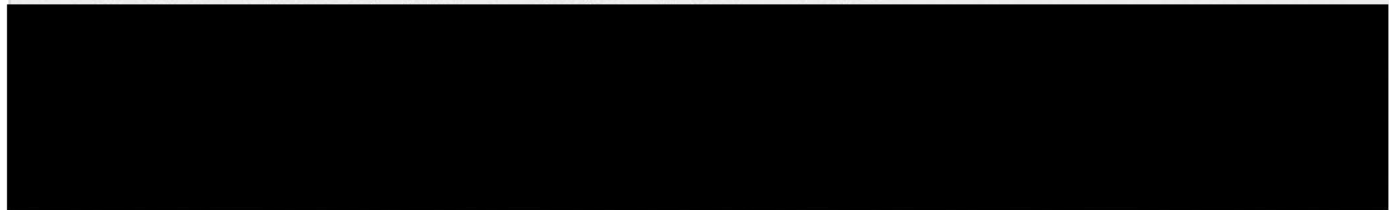
Baseline management including:

- 1) Operating system/firmware
- 2) Software version
- 3) Logical network accessible ports
- 4) Security patches
- 5) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

The likelihood that this event would adversely impact the Bulk Electric System is considered minimal because:



Additional Comments:

This violation was not the result of intentional action to violate a NERC reliability standard. was attempting to comply in good faith with the applicable NERC reliability standard at issue in this potential violation. The internal compliance plan was in effect at the time of the potential noncompliance. management relevant to the situation actively participated and encouraged employees to provide complete information.

There have been no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance.

Attachment 27

Record documents for the violation of CIP-007-3a R3

27.a The Companies' Self-Report [REDACTED]

27.b The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 4/13/2016

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: CIP-007-3a

Applicable Requirement: R3.

Applicable Sub Requirement(s): R3.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

9/16/2014

Monitoring Method for previously reported or discovered:

Self-Certification

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: 1/19/2016

Beginning Date of Possible Violation: 9/16/2015

End or Expected End Date of Possible Violation: 2/25/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report involves [REDACTED]

Per CIP-007-3, R3, [REDACTED] is obligated to either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

On Jan 19, 2016 during a quality assurance (QA) spot check of monitoring for [REDACTED] security patch assessments, the CIP Point of Contact (CPOC) for [REDACTED] identified that [REDACTED] security patch assessments appeared to be out of date. After further research, it was confirmed on 2/3/2016, that the process for performing [REDACTED] security patch assessments was not being followed.

There were [REDACTED] security vulnerability notifications (including duplicate notifications) received that were not assessed; all vulnerability notifications have now been assessed for applicability to the NERC-CIP environment.

Of the [REDACTED] security vulnerability notifications received since September 16, 2015, there were [REDACTED] patch assessments not evaluated within the 30 day window.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

Assessing the [REDACTED] security patch notifications in a timely manner has been reinforced.

One-on-one counseling with employees has occurred.

All [REDACTED] security patch notifications not previously assessed have been identified.

All [REDACTED] security patch notifications not previously assessed have been assessed and all others since that time.

Training of The [REDACTED] has occurred.

Two individuals have now been assigned to monitor and assess the [REDACTED] alerts (instead of one).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide details to prevent recurrence:

The actions that [REDACTED] is taking include:

- Provide training on the [REDACTED]
- Identify all missed [REDACTED] security patch notifications
- Assess all missed [REDACTED] security patch notifications
- Document all missed [REDACTED] security patch notifications
- Document all future assessments of [REDACTED] security patch notifications and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
- Eliminate single point of failure

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

2/25/2016

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:

The Potential Impact to the Bulk Power System is minimal. Due to the logical location of network switches and the system hardening, exposure of unpatched vulnerabilities present a minimal potential risk. No events have been identified due to patching issues.

Provide detailed description of Actual Risk to Bulk Power System:

The Actual Impact to the Bulk Power System is minimal because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

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.)

This item was submitted by [REDACTED] on [REDACTED]

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: CIP-007-3a

Applicable Requirement: R3.

Applicable Sub Requirement(s): R3.1.; R3.2.

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: [REDACTED]

Beginning Date of Possible Violation: 8/15/2015

End or Expected End Date of Possible Violation: 10/28/2016

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

During audit preparation review sessions in [REDACTED] it was determined that IT failed to monitor vendor security patches and vulnerability notifications at least once every 30 calendar days as required by CIP Version 3 for the 12 [REDACTED] devices listed below. The [REDACTED] team has a patch management process but does not include monitoring for [REDACTED] devices. During the [REDACTED] it was decided that [REDACTED] would monitor vendor security patches and vulnerability notifications for [REDACTED] devices. When security patches and vulnerability notifications were identified, [REDACTED] would notify [REDACTED] who would be responsible for installing the patches. Unfortunately, this did not transpire. Twelve (12) devices are impacted for this possible violation. These twelve (12) devices have never been patched since being deployed. The devices are six (6) [REDACTED] and six (6) [REDACTED]. The time frame for the assessment associated with this [REDACTED] is August 15, 2015 which was when the assets were transferred to [REDACTED] to manage the patching of the systems until January 30, 2016 which was the last date that [REDACTED] planned any possible maintenance release or scheduled software remedy for a security vulnerability issue.

The total number of possible vulnerabilities analyzed = [REDACTED] which were identified through the [REDACTED] and the [REDACTED] webpage. [REDACTED] security vulnerabilities were identified as being applicable [REDACTED] applicable to [REDACTED] sets of [REDACTED] and the [REDACTED] applicable to the [REDACTED]. The severity ratings of the applicable security vulnerabilities are [REDACTED] high [REDACTED] and [REDACTED] medium [REDACTED]. These security vulnerabilities have not been installed as the risk to [REDACTED] is low based on the existing layered security controls in place for the [REDACTED] networks. There is a patch mitigation plan that will have these devices decommissioned. The devices are in the process of being decommissioned, which has already started with the [REDACTED] assets. The decommissioning of the [REDACTED] assets will start after the [REDACTED] project, which is in Q2, 2018; therefore, the goal is not to update the devices, because updating introduces a certain degree of risk that the business would like to avoid.

[REDACTED]

[REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

There is a patch mitigation plan that will have these devices decommissioned. The devices are in the process of being decommissioned, which has already started with the [REDACTED] assets. The decommissioning of the [REDACTED] assets will start after the [REDACTED] project, which is in Q2, 2018

Provide details to prevent recurrence:

This possible violation has been added to the RCA for [REDACTED] which will assist in creating a plan to prevent recurrence

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

6/30/2017

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:

The Potential Impact to the Bulk Power System is minimal as the systems in the current state are stable and applying the patches could make the systems unstable. Also, the [REDACTED] network is isolated and prohibits remote access. The fact that the network topology/infrastructure is not public or well-known and cannot be scanned from the internet assist with keeping the impact to the Bulk Power System minimal.

Provide detailed description of Actual Risk to Bulk Power System:


There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

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.)

Attachment 28

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

28.a The Companies' Self-Report 

This item was submitted by [REDACTED] on 9/5/2017

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: CIP-007-6

Applicable Requirement: R3.

Applicable Sub Requirement(s): 3.3.

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: 5/12/2017

Beginning Date of Possible Violation: 12/1/2016

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:

This self-report is for [REDACTED]

CIP-007 R3 requires a process for updating Anti-Virus signatures. For [REDACTED] that process is [REDACTED]. R3.3 is specific to AV signature updates and the process that is followed. [REDACTED] requires a 35-day monitoring cycle. To evidence compliance with [REDACTED] and ultimately CIP-007 R3, evidence of the checks for updates and the application of those updates is required.

During an internal assessment, it was identified that six months (December 2016-May 2017) of AV documentation for the Medium network at [REDACTED] was missing.

Further investigation of the other two medium cyber systems located at [REDACTED] sites yielded no evidence of missing documentation - [REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Anti-Virus updates have been completed with documentation

Provide details to prevent recurrence:

To prevent recurrence, [REDACTED] has implemented stronger task execution and oversight controls as part of the overall program including:

Ongoing [REDACTED] were added for Monthly Compliance Activities

[REDACTED] Oversight Execution Tasks were added for [REDACTED] to complete Activity Oversight for compliance activities

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

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

6/16/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal [REDACTED]

Actual Impact to the Bulk Power System: Minimal [REDACTED]

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because this was a documentation error. The signatures were applied on schedule, but there is no evidence to show application.

Provide detailed description of Actual Risk to Bulk Power System:

The Actual Impact to the Bulk Electric System is minimal. There was no Actual Impact to the Bulk Power System caused by this potential violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this violation.

Additional Comments:

Root cause analysis was performed at the [REDACTED] and a mitigation plan will be developed at the [REDACTED] to address identified root causes.

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.)

Attachment 29

Record documents for the violation of CIP-007-6 R4

29.a The Companies' Self-Report [REDACTED]

29.b The Companies' Self-Report [REDACTED]

29.c The Companies' Self-Report [REDACTED]

29.d The Companies' Self-Report [REDACTED]

29.e Audit Summary [REDACTED]

This item was submitted by [REDACTED] on 9/13/2017

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: CIP-007-6

Applicable Requirement: R4.

Applicable Sub Requirement(s): 4.1.

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: 9/12/2016

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 9/15/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-007-6 R4.1, [REDACTED] is obligated to log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

- 4.1.1. Detected successful login attempts;
- 4.1.2. Detected failed access attempts and failed login attempts;
- 4.1.3. Detected malicious code.

While performing internal review of documentation on September 12, 2016, a [REDACTED] compliance monitor requested security event logs for [REDACTED] Medium Impact BES Cyber Assets (BCA). [REDACTED] each at [REDACTED]. The [REDACTED] are [REDACTED]. It was discovered that the logs were not available and the security event logging was not configured on the three BCAs. The [REDACTED] sampled BCAs were made by [REDACTED] and [REDACTED] configured as [REDACTED].

Causes of the violation

Apparent Cause #1 Lack of procedures
No procedures outlining CIP-V5 requirements or how to develop compliant [REDACTED] settings were in place when the [REDACTED] settings were developed and commissioned.

Apparent Cause #2 Lack of compliance verification There was no verification of compliance performed on the [REDACTED] when it was installed since it was installed prior to the CIP-V5 effective date. A prior project determined what existing assets needed to be compliant on the effective date but this [REDACTED] was installed at a later date. No additional compliance verification of existing assets was performed prior to the effective date. Also, there is minimal guidance on what evidence is needed to prove compliance and how this evidence verified once it is obtained.

Contributing Cause #1 Insufficient Change Management

A change management process was put in place to disseminate the requirements of the new CIP-V5 standard. However, this information was only given to management level individuals. As critical as compliance is to [REDACTED] the team believes individual contributors should be included in this change management process.

During the extent of condition review in all four [REDACTED] BCAs were identified as not having logging configured at the Cyber Asset Level and did not generate logs for the event types required per cyber asset capability. The extent of condition did not identify any issues in [REDACTED] or [REDACTED].

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Logging configuration updates were tested in a lab environment. The following [REDACTED] devices were updated and confirmed to be logging events:

Location Date

[REDACTED]
[REDACTED]
[REDACTED]

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include the following:

- 1) Update configurations and verify logging on devices identified in the extent of condition. Due Date: 9/15/17
- 2) Create a job aid/ guidance document for [REDACTED] that outlines the current requirements and interpretations for NERC CIP Standards CIP007. Due Date: 9/30/17
- 3) Create a procedure that outlines how to develop device settings for [REDACTED] to verify all NERC CIP compliance requirements are met. Due Date: 10/31/17
- 4) Create a Job Aid for field personnel that outlines the process for commissioning a NERC CIP [REDACTED] and how to obtain evidence to verify compliance. Due Date: 10/31/17
- 5) Review the causal factors from this potential violation and discuss the findings and the newly created procedures and documents with employees (Compliance, Engineering, [REDACTED] Field personnel) at a future staff meeting. Due Date: 11/15/2017

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

[REDACTED]

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal [REDACTED]

Actual Impact to the Bulk Power System: Minimal [REDACTED]

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is moderate because:

- 1) A cyber security incident has not been reported at any medium impact BES asset listed in the extent of condition.
- 2) Records of logs used to identify a cyber security incident where not available.
- 3) Records of logs can identify detected malicious code. The [REDACTED] have [REDACTED] installed. [REDACTED] is a whitelisting application that deters malicious code. The programs present in an [REDACTED] update package, in an un-modified state, are allowed to execute. Whitelist inspects a program's binary image before it is allowed to execute, verifying its legitimacy and integrity against a known signature created at build time. This would deter or prevent malicious code on the devices using [REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

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.)

This item was submitted by [REDACTED] on 4/7/2017

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: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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: 1/5/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 1/11/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

- a. [REDACTED]
- b. [REDACTED]
- c. [REDACTED]

The devices [REDACTED] reside in the [REDACTED] and the following number of devices are with this BCS:

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Yes, these devices were reclassified as follows:

- a. [REDACTED] - 74357 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- b. [REDACTED] - 74363 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- c. [REDACTED] - 74355 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17

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

Provide details to prevent recurrence:

A cause analysis will be performed to evaluate additional causal factors to identify effective corrective actions to prevent reoccurrence.

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

1/11/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal [REDACTED]

Actual Impact to the Bulk Power System: Minimal [REDACTED]

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

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.)

This item was submitted by [REDACTED] on 1/23/2018

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

4/7/2017

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: Yes

If yes, indicate which Region(s):

[REDACTED]

Date Reported to Region(s):

4/7/2017

Date Possible Violation was discovered: 11/15/2017

Beginning Date of Possible Violation: 11/15/2017

End or Expected End Date of Possible Violation: 11/17/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED] and [REDACTED]

Per CIP002-5, R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

Per sub-requirement R1.1:

Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

Problem Statement

[REDACTED] were not properly classified as High Impact Electronic Access Control or Monitoring Systems (EACMS), causing the devices to potentially not have full North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), resulting in this possible violation.

Additional Information:

Categorization of Bulk Electric System (BES) Cyber Assets (CAs), BCAs, is the process whereby a CA and then assigns the appropriate categorization to that device. Proper categorization of EACMS ensures appropriate NERC CIP protections are implemented on the identified asset.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

[Redacted]

[Redacted]

Method of Discovery

Self-Assessment: [Redacted]

[Redacted]

Extent Of Condition:

As part of the [Redacted] the [Redacted] will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all [Redacted] will need to 1) reassess their technologies to ensure alignment with the [Redacted] and 2) ensure [Redacted] processes support the new program which may require the [Redacted] to work through the asset classification process for all assets under the revised program.

Cause Analysis:

This violation occurred as a result of:

- Lack of specificity within the [Redacted] requirements of the process, no process available.

Cause Identification:

- Prior self-reported issues with [Redacted] and other firewall rules focused on systems designed to facilitate [Redacted] were incorrectly implemented due to the lack of clarity in the [Redacted]
- [Redacted] and [Redacted] were not properly assessed in the V5 transition as being Intermediate Systems
- [Redacted] and [Redacted] were not previously identified as EACMS because their primary function was not to enable remote access

The direct and contributing causes of this possible violation:

Apparent Cause 1 (AC1): Process Weakness. Lack of specificity within the [Redacted] requirements of the process; no process available.

Prior self-reported issues with [Redacted] focused on systems designed to facilitate [Redacted] and were incorrectly implemented due to the lack of clarity during the implementation of the [Redacted]

[Redacted]

Are Mitigating Activities in progress or completed? Yes

[An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.](#)

If Yes, Provide description of Mitigating Activities:

Actions [Redacted] has already completed to remediate this potential violation include:

On 11/28/2017, [Redacted] determined this violation a self-report and the [Redacted] team submitted the appropriate [Redacted] workflow to correctly update the categorization and create the necessary work orders to apply the appropriate controls to the identified devices.

Completed: As of 12/4/2017, all identified devices have been re-categorized as EACMS.

Provide details to prevent recurrence:

██████████ has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that ██████████ will incur further risk of the same or similar NERC reliability standard violation.

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE. THIS INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

See section 7.0 Corrective Actions (Fixes) Recommended by Cause Analysis Team for respective milestone dates.

- CIP-002 ██████████ Refresh. ██████████ to provide updated CIP-002 ██████████ documentation that will be used by all ██████████ to perform a gap analysis and re-evaluation of in-scope BES Cyber Assets
- With oversight from ██████████ all ██████████ to perform a business procedure / gap analysis between the current CIP-002 / ██████████ business procedures and the updated CIP-002 / ██████████ documentation
- With oversight from ██████████ all ██████████ to provide a draft of CIP-002 / ██████████ business level procedures
- With oversight from ██████████ all ██████████ to obtain ██████████ business level procedures approved
- With oversight from ██████████ all ██████████ to identify those individuals who require training on updated CIP-002 / ██████████ business level procedures
- With oversight from ██████████ all ██████████ to communicate and provide training on updated CIP-002 / ██████████ business level procedures to those individuals requiring training
- With oversight from ██████████ all ██████████ to re-evaluate / re-classify BES Cyber Assets based on updated business level procedures and submit potential violation if identified
- ██████████ to submit ██████████ tickets to initiate workflow necessary to re-classify identified devices as EACMS
- ██████████ to perform an active review of All ██████████ to determine if any additional systems have been improperly classified
- ██████████ to submit ██████████ tickets to push firewall rules for scanning identified devices
- ██████████ to perform security controls testing (SCT) on identified devices

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

11/28/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

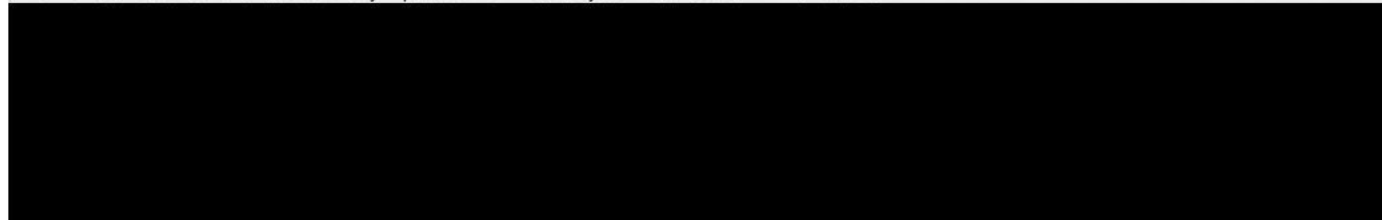
Baseline management including:

- 1) Operating system/firmware
- 2) Software version
- 3) Logical network accessible ports
- 4) Security patches
- 5) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

██████████ did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

The likelihood that this event would adversely impact the Bulk Electric System is considered minimal because:



Additional Comments:

This violation was not the result of intentional action to violate a NERC reliability standard. ██████████ was attempting to comply in good faith with the applicable NERC reliability standard at issue in this potential violation. The ██████████ internal compliance plan was in effect at the time of the potential noncompliance. ██████████ management relevant to the situation actively participated and encouraged employees to provide complete information.

There have been no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance.

This item was submitted by [REDACTED] on 11/27/2017

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

4/7/2017

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: 8/1/2017

Beginning Date of Possible Violation: 5/5/2017

End or Expected End Date of Possible Violation: 8/8/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

During a meeting between a [REDACTED] a concern was raised that [REDACTED] was not categorized correctly in the [REDACTED]. After further investigation it was determined that the associated server [REDACTED] was categorized correctly, however, the associated [REDACTED] was categorized as "No Tier".

August 8, 2017:

[REDACTED] was submitted for the re-assessment of [REDACTED] and to apply the appropriate controls for a BES Cyber Asset.

Cause Analysis:

- [REDACTED] does not have a mechanism built into the tool (technical control) to ensure proper ticket categorization of BCAs.
- A manual review of [REDACTED] will not prevent the ticket from being classified as "No Tier" and closed when the BCA has an IP address on an ESP Network.

Extent Of Condition:

The extent of condition analysis for this potential violation originally focused on the [REDACTED] used by [REDACTED] to manage NERC CIP assets. [REDACTED] does not use any other asset management tool, such as [REDACTED], to manage NERC CIP assets, where this condition might occur.

A further extent of condition was performed for all other applicable business units to determine if the potential for an asset classification violation could exist in their respective area.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Conclusion:

[REDACTED]

[REDACTED] has previously reported this violation and corrective actions were completed. See [REDACTED]

[REDACTED]

[REDACTED] - The annual Cyber Vulnerability Assessment review concluded that devices had incorrect NERC CIP Classification assigned.

See [REDACTED]

[REDACTED] Has identified several cases where devices were incorrectly classified as Medium when they should have been classified as Low. This "administrative" error did not result in a potential violation.

[REDACTED]

As part of the PSP commissioning process [REDACTED] ensures the [REDACTED] are enabled and operating effectively. As part of this [REDACTED] adds this asset to the [REDACTED] listing in the [REDACTED] is dependent on the Business Area (owner of the location) to classify the type of PSP they need (High, Med w/ERC, Med wo/ERC). EPS does not perform this classification but implements the required processes based on the Business Unit determination. [REDACTED]

No CIP002-5 R1 issues identified.

[REDACTED]

No CIP002-5 R1 issues identified.

[REDACTED]

[REDACTED] Through this collaboration the proper categorization is determined.

No CIP002-5 R1 issues identified.

[REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System:

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

Baseline management including:

- 3) Operating system/firmware
- 4) Software version
- 5) Logical network accessible ports
- 6) Security patches
- 7) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

[REDACTED] did not identify any actual impact to the Bulk Electric System as a result of this potential violation.

[REDACTED] considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

[REDACTED]

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 I, Section 6.4.)

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

Post On-site Audit/Off-site Audit/Spot Check/Investigation Screening Worksheet

Prepared By: [REDACTED]

Submittal Date: [REDACTED]

Compliance Monitoring Method (On-site Audit, Off-site Audit, Spot-Check, or Investigation):
On-Site Audit

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

Registered Entity Contact Information:

Name: [REDACTED]

Email: [REDACTED]

Standard: CIP-007-6

Requirement: R4

Sub Requirement(s): R4.4

Function(s) Applicable to Possible Violation:

[REDACTED]

Date violation occurred: 07/01/2016

Date violation discovered (Exit Presentation Date): [REDACTED]

Is the violation still occurring? Yes No

Are mitigating activities (including details to prevent reoccurrence) in progress or completed? Yes No

If yes, Provide description of Mitigating Activities:

Date Mitigating Activities are expected to be completed or were completed:

Detailed explanation and cause of violation: While on-site, the audit team discovered that [REDACTED] failed to review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.

[REDACTED] High Impact BES Cyber Systems and their associated EACMS and PCAs, did not have their 15 day log summarization review or sampling of logged events completed for [REDACTED] assets. Approximately [REDACTED] Cyber Assets are impacted.

Potential Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

Actual Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

Detailed description of Potential Risk to Bulk Power System: Minimal potential impact to the BPS due to other controls observed in place. Also, the entity immediately reviewed the logs for the subsequent time interval.

Detailed description of Actual Risk to Bulk Power System: There was Minimal Impact to the Bulk Power System caused by this possible violation. This determination is due to the fact that no actual event or adverse consequences occurred.

Additional Comments: Reference Information: [REDACTED]
[REDACTED]

Please complete the form as completely as possible and email to [REDACTED]

Attachment 30

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

30.a The Companies' Self-Report [REDACTED]

30.b The Companies' Self-Report [REDACTED]

30.c The Companies' Self-Report [REDACTED]

30.d The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 8/29/2016

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: CIP-007-3a

Applicable Requirement: R5.

Applicable Sub Requirement(s): R5.1.

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: 5/12/2016

Beginning Date of Possible Violation: 5/9/2016

End or Expected End Date of Possible Violation: 5/12/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This applies to :
Unauthorized Electronic Access (CIP-007-3 R5.1.1)

On May 9, 2016, a [REDACTED] manager was informed by a [REDACTED] service technician that he had been sharing his electronic account information (username and password) with team members who did not have authorized access to BES Cyber Assets at a [REDACTED]. On May 12, the manager immediately banned the sharing of individual account information. In parallel, the manager requested the [REDACTED] Lead begin the process of identifying and requesting authorization for the individuals who required access. This process consisted of processing their background checks and training if it had not already been performed.

The initial investigation of what happened revealed the devices in question were previously accessible via a shared-use account. However, a system upgrade on 8/28/13 replaced the shared use access with individual accounts and not all [REDACTED] service technicians were alerted of the change.

After the upgrade, one [REDACTED] technician was set up with individual account access. He shared this access with two teammates in order to facilitate service response and routine activities. The two [REDACTED] technicians had completed their PRA and required NERC CIP training prior to the upgrade but a user account had not been requested for each of them. The two teammates had NERC CIP physical access to the site just not electronic access. [REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Provide details to prevent recurrence:

- The actions that [REDACTED] taking to prevent recurrence include the following:
- Employees requiring access to devices will be required to complete a PRA and Training
 - [REDACTED] will follow [REDACTED] prescribed process for requesting individual accounts to gain access.
 - [REDACTED] will take an action to develop and deliver training to prevent this from occurring in other [REDACTED]

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

9/30/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
			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:

The Potential Impact to the Bulk Power System is minimal. The two [REDACTED] technicians who were given electronic account information had been NERC CIP qualified with having completed the required PRA and training. The two techs had been able to access the devices prior to the system upgrade. After the system upgrade on 8/28/13 replaced the shared use access with individual accounts, not all [REDACTED] service technicians were alerted of the change. The electronic account information was shared to allow the two technicians to have the ability to facilitate service responses and routine activities. Mitigating actions were the immediate banning of the sharing of individual account information, as well as a request to the [REDACTED] Lead to begin the process of identifying and requesting authorization for the individuals who required access.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation. The two technicians that were given the shared electronic account information used that information to perform routine service activities only. There was no intent to violate any NERC standards.

Additional Comments:

This potential violation was not the result of intentional action to violate a NERC reliability standard.
[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

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.)

This item was submitted by [REDACTED] on [REDACTED]

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: CIP-007-6

Applicable Requirement: R5.

Applicable Sub Requirement(s): 5.2.

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: 8/16/2016

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 8/16/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Self report applies to [REDACTED]

CIP-007-5 R5.2. requires [REDACTED] to 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). This standard and requirement are to have been met by the date of July 1, 2016

[REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation. The [REDACTED] internal compliance plan that was in effect at the time of the potential noncompliance.

There were no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance
ASSOCIATED RECORD AND REGION INFORMATION

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.)

This item was submitted by [REDACTED] on 9/22/2015

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: CIP-007-3a

Applicable Requirement: R5.

Applicable Sub Requirement(s): R5.3.

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): [REDACTED]

Date Reported to Region or Discovered by Region: 12/19/2012

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: 4/29/2015

Beginning Date of Possible Violation: 12/31/2014

End or Expected End Date of Possible Violation: 8/1/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per NERC CIP Requirements CIP-007-3a; R5.3.3, [REDACTED] is obligated to change passwords at least annually or more frequently based on risk.

On April 29, 2015, a relay tech identified that a password on a [REDACTED] device, [REDACTED] was not changed during the Annual Password change procedure at [REDACTED]. This device had 7 accounts with different levels of permission. Level 1 was the Read Only permission level which was the only Password that was not changed.

Only the device at [REDACTED] has been identified as not having the password changed. If more devices had been missed, the Engineering staff would have known on the day the changes were made because the level one password is needed for [REDACTED] to be passed back to the [REDACTED] where the [REDACTED] is the source for [REDACTED] data. The log generated through [REDACTED] is used to show evidence of password changes made remotely. If there were another device without a password change, the log would show this, as well as other locations with the same issue.

The work request was generated in the [REDACTED] database to make the password setting changes by year end.

Upon further investigation as to why the password change did not happen, it was determined the 'Save' function did not execute as intended when the password change was originally attempted.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

This violation was mitigated by changing the password on that particular relay at [REDACTED] and verified on 6/29/15.

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include the following:

A control has been created that requires two people review the password change as it is being made. Another control has also been established which randomly tests passwords to make sure they have been changed.

The procedure of password changes includes logging back in (randomly) once the password has been changed. This information is captured in the [REDACTED] log file

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

8/1/2015

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:

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because the password did not allow for administrative level access. Additionally, there were no misoperations, emergencies or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

The [REDACTED] internal compliance plan that was in effect at the time of the potential noncompliance could not have prevented the potential noncompliance, due to the misoperation of the Save function which did not execute as intended when the Password change was originally attempted.

The system was within a defined ESP and PSP where physical and electronic access is monitored.

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.)

This item was submitted by [REDACTED] on 9/5/2017

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: CIP-007-3a

Applicable Requirement: R5.

Applicable Sub Requirement(s): R5.2.; R5.3.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

[REDACTED]

Monitoring Method for previously reported or discovered:

Spot-Check

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: 2/20/2017

Beginning Date of Possible Violation: 3/31/2016

End or Expected End Date of Possible Violation: 3/31/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-007-6; R5.4, R5.5, [REDACTED] is obligated to perform password changes on BES Cyber Asset from manufacturer default and at least once every 15 calendar months.

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:

- Upon discovery, the missed passwords were updated to meet complexity requirements.
- [REDACTED] will formally document the password QA process for devices that are remotely accessible
- [REDACTED] will formally document a Password QA process for field applied passwords

Additional mitigating activities are scheduled and will extend into 2018.

Provide details to prevent recurrence:

A full enterprise wide mitigation plan for [REDACTED] is being developed to prevent this issue from recurring. The Mitigation Plan includes developing procedures, documents, and formal training.

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

11/30/2017

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:

The Potential Impact to the Bulk Power System is minimal because the device is protected within a PSP (Physical Security Perimeter) for Physical Access, as well as an ESP (Electronic Security Perimeter).

All the technicians who were responsible for the Annual Password changes had completed a PRA and NERC CIP training.

Upon discovery, the password was changed immediately.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

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.)

Attachment 31

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

31.a The Companies' Self-Report [REDACTED]

31.b The Companies' Self-Report [REDACTED]

31.c The Companies' Self-Report [REDACTED]

31.d The Companies' Self-Report [REDACTED]

31.e The Companies' Self-Report [REDACTED]

31.f The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 7/19/2017

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: CIP-007-6

Applicable Requirement: R5.

Applicable Sub Requirement(s): 5.7.

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: 5/3/2017

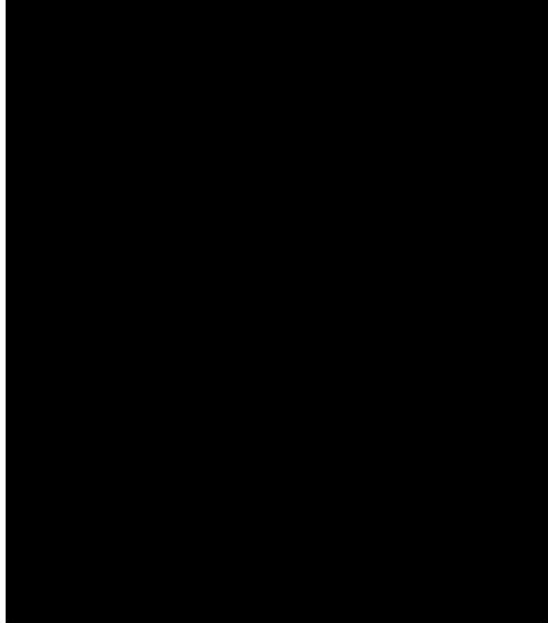
Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 9/29/2017

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:
This Self-Report applies to [REDACTED]

[REDACTED]

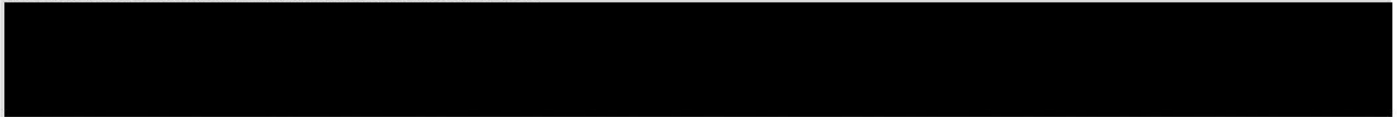


Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:



Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

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.)

This item was submitted by [REDACTED] on 4/7/2017

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: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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: 1/5/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 1/11/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Yes, these devices were reclassified as follows:

- a. [REDACTED] - 74357 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- b. [REDACTED] - 74363 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- c. [REDACTED] - 74355 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17

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

Provide details to prevent recurrence:

A cause analysis will be performed to evaluate additional causal factors to identify effective corrective actions to prevent reoccurrence.

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

1/11/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal [REDACTED]

Actual Impact to the Bulk Power System: Minimal [REDACTED]

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

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.)

This item was submitted by [REDACTED] on 1/23/2018

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

4/7/2017

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: Yes

If yes, indicate which Region(s):

[REDACTED]

Date Reported to Region(s):

4/7/2017

Date Possible Violation was discovered: 11/15/2017

Beginning Date of Possible Violation: 11/15/2017

End or Expected End Date of Possible Violation: 11/17/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP002-5, R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

Per sub-requirement R1.1:

Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

Problem Statement

[REDACTED] were not properly classified as High Impact Electronic Access Control or Monitoring Systems (EACMS), causing the devices to potentially not have full North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), resulting in this possible violation.

Additional Information:

Categorization of Bulk Electric System (BES) Cyber Assets (CAs), BCAs, is the process whereby a CA and then assigns the appropriate categorization to that device. Proper categorization of EACMS ensures appropriate NERC CIP protections are implemented on the identified asset. PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

[REDACTED]

Method of Discovery

Self-Assessment: [REDACTED]

[REDACTED]

Extent Of Condition:

As part of the [REDACTED] the [REDACTED] group will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all [REDACTED] will need to 1) reassess their technologies to ensure alignment with [REDACTED] and 2) ensure [REDACTED] Level processes support the new program which may require the [REDACTED] to work through the asset classification process for all assets under the revised program.

Cause Analysis:

This violation occurred as a result of:

- Lack of specificity within [REDACTED] requirements of the process, no process available.

Cause Identification:

- Prior self-reported issues with [REDACTED] focused on systems designed to facilitate IRA were incorrectly implemented due to the lack of clarity in the [REDACTED]
- [REDACTED] were not properly assessed in the V5 transition as being Intermediate Systems
- [REDACTED] were not previously identified as EACMS because their primary function was not to enable remote access


The direct and contributing causes of this possible violation:

Apparent Cause 1 (AC1): Process Weakness. Lack of specificity within the [REDACTED] requirements of the process; no process available.

Prior self-reported issues with [REDACTED] focused on systems designed to facilitate IRA and were incorrectly implemented due to the lack of clarity during the implementation of the [REDACTED] program.

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Actions [REDACTED] has already completed to remediate this potential violation include:

On 11/28/2017, [REDACTED] determined this violation a self-report and [REDACTED] submitted the appropriate [REDACTED] workflow to correctly update the categorization and create the necessary work orders to apply the appropriate controls to the identified devices.

Completed: As of 12/4/2017, all identified devices have been re-categorized as EACMS.

Provide details to prevent recurrence:

██████████ has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that ██████████ will incur further risk of the same or similar NERC reliability standard violation. **PROTECTED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

See section 7.0 Corrective Actions (Fixes) Recommended by Cause Analysis Team for respective milestone dates.

- CIP-002 ██████████ to provide updated CIP-002 ██████████ documentation that will be used by all ██████████ to perform a gap analysis and re-evaluation of in-scope BES Cyber Assets
- With oversight from ██████████ all ██████████ to perform a business procedure / gap analysis between the current CIP-002 / ██████████ business procedures and the updated CIP-002 ██████████ documentation
- With oversight from ██████████ all ██████████ to provide a draft of CIP-002 ██████████ business level procedures
- With oversight from ██████████ all ██████████ to obtain ██████████ business level procedures approved
- With oversight from ██████████ all ██████████ to identify those individuals who require training on updated CIP-002 ██████████ business level procedures
- With oversight from ██████████ all ██████████ to communicate and provide training on updated CIP-002 ██████████ business level procedures to those individuals requiring training
- With oversight from ██████████ all ██████████ to re-evaluate / re-classify BES Cyber Assets based on updated business level procedures and submit potential violation if identified
- ██████████ to submit ██████████ to initiate workflow necessary to re-classify identified devices as EACMS
- ██████████ to perform an active review of All ██████████ Management Systems to determine if any additional systems have been improperly classified
- ██████████ to submit ██████████ to push firewall rules for scanning identified devices
- ██████████ to perform security controls testing (SCT) on identified devices

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

11/28/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

Baseline management including:

- 1) Operating system/firmware
- 2) Software version
- 3) Logical network accessible ports
- 4) Security patches
- 5) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

██████████ did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

The likelihood that this event would adversely impact the Bulk Electric System is considered minimal because:



Additional Comments:

This violation was not the result of intentional action to violate a NERC reliability standard. ██████████ was attempting to comply in good faith with the applicable NERC reliability standard at issue in this potential violation. The ██████████ internal compliance plan was in effect at the time of the potential noncompliance. ██████████ management relevant to the situation actively participated and encouraged employees to provide complete information.

There have been no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance.

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

This item was submitted by [REDACTED] on 11/27/2017

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

4/7/2017

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: 8/1/2017

Beginning Date of Possible Violation: 5/5/2017

End or Expected End Date of Possible Violation: 8/8/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

During a meeting [REDACTED] a concern was raised that [REDACTED] was not categorized correctly in the [REDACTED]. After further investigation it was determined that the associated server [REDACTED] was categorized correctly, however, the associated [REDACTED] was categorized as "No Tier".

August 8, 2017:

[REDACTED] ticket was submitted for the re-assessment of [REDACTED] and to apply the appropriate controls for a BES Cyber Asset.

Cause Analysis:

[REDACTED]

Extent Of Condition:

[REDACTED]

A further extent of condition was performed for all other applicable business units to determine if the potential for an asset classification violation could exist in their respective area.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Conclusion:

[REDACTED]

[REDACTED] has previously reported this violation and corrective actions were completed. See [REDACTED]

[REDACTED]

[REDACTED] The annual Cyber Vulnerability Assessment review concluded that devices had incorrect NERC CIP Classification assigned.

See [REDACTED]

[REDACTED] Has identified several cases where devices were incorrectly classified as Medium when they should have been classified as Low. This "administrative" error did not result in a potential violation.

[REDACTED]

As part of the PSP commissioning process [REDACTED] ensures the PACS [REDACTED] are enabled and operating effectively. As part of this [REDACTED] adds this asset to the [REDACTED] listing in [REDACTED] is dependent on the Business Area (owner of the location) to classify the type of PSP they need (High, Med w/ERC, Med wo/ERC).

No CIP002-5 R1 issues identified.

[REDACTED]

This support group is no longer performing asset classification. All new assets that support EMS are being managed by the [REDACTED] organization and follow [REDACTED] asset classification processes.

No CIP002-5 R1 issues identified.

[REDACTED]

Both support groups collaborate with [REDACTED] lead to verify the location and function of the device being categorized. Through this collaboration the proper categorization is determined.

No CIP002-5 R1 issues identified.

Associated Asset [REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System:

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

Baseline management including:

- 3) Operating system/firmware
- 4) Software version
- 5) Logical network accessible ports
- 6) Security patches
- 7) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

[REDACTED] did not identify any actual impact to the Bulk Electric System as a result of this potential violation.

[REDACTED] considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

[REDACTED]

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 I, Section 6.4.)

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

This item was submitted by [REDACTED] on 11/28/2017

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: CIP-007-6

Applicable Requirement: R5.

Applicable Sub Requirement(s): 5.2.

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: 7/1/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 4/16/2018

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report to [REDACTED]

During the first annual performance of the Cyber Vulnerability Assessments, [REDACTED] discovered possible violations of a Reliability Standard Requirement. [REDACTED] discovered a number of issues with undocumented enabled default and/generic accounts. This includes default manufacturer accounts not documented or inaccurately documented on the System Security Baselines (SSB).

[REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Severe

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The actions that [REDACTED] is taking to prevent recurrence include the following:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

[REDACTED]

[REDACTED] is required before access to the end system is possible. As a result of these controls, there was no actual impact to the Bulk Electric System caused by this possible violation and no misoperations, emergencies, or other adverse consequences to the Bulk Electric System occurred.

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.)

This item was submitted by [REDACTED] on 6/19/2017

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: CIP-007-6

Applicable Requirement: R5.

Applicable Sub Requirement(s): 5.6.

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: 5/22/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 6/8/2017

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This applies [REDACTED]
 Per CIP-007-6 R5.6, where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.
 On May 23, 2017, during [REDACTED] Paper Vulnerability Assessment activity, it was discovered that local accounts were not being managed by [REDACTED]. The [REDACTED] hosts included [REDACTED]

[REDACTED]

Future mitigating activities include working with the vendor, [REDACTED] to reset or replace the failing [REDACTED] with a like-for-like asset. Anticipated completion date is June 23, 2017.

A Cause Analysis will be performed which will include a mitigation plan to remediate the causes of the potential violation.

[REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no actual impact to the Bulk Power System as a result of this potential violation.

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.)

Attachment 32

Record documents for the violation of CIP-007-3a R6

32.a Audit Summary



[REDACTED]

Possible Violation (PV) / Find, Fix, and Track (“FFT”) Identification Form

This document is to be completed upon identification of a possible violation (PV), typically within 5 business days of the audit exit brief and emailed to [REDACTED] with a copy to [REDACTED]

For non-FFT candidates: Upon receipt of this document, Enforcement will coordinate with the reporting auditor and Enforcement to initiate the Enforcement processing of this possible violation.

Violation Reported By: [REDACTED]

Submittal Date: [Click here to enter text.](#)

Candidate for FFT Treatment: YES NO

Registered Entity: [REDACTED]

NERC Registry ID#: [REDACTED]

Compliance Monitoring Process: Compliance Audits

Standard, Version and Requirement in Violation: CIP-007-3a, R6

Registered Function(s) in Violation: [REDACTED]

Initial PV Date (Actual Date Discovered by) [REDACTED]

Date for Determination of Penalty/Sanction (Beginning Date of Violation): 4/30/2015

End Date of Possible Violation: 11/11/2015

For Non-FFT Candidate ONLY

Violation Risk Factor: VRF - Medium

Violation Severity Level: Severe VSL

[REDACTED]

Potential Impact to Bulk Electrical System (BES): Minimal

Provide Explanation for Selection:

[REDACTED] did not ensure that security monitoring controls to generate alerts for unsuccessful login thresholds were properly implemented for [REDACTED] devices (a mixture of CCAs, EACMs, etc). The root cause is defined as a monitoring system configuration issue.

For Non-FFT and FFT Candidates

Basis for the PV:

The audit team finds a possible violation for CIP-007-3 R6 (R6.2) as [REDACTED] did not ensure that security monitoring controls to generate alerts for unsuccessful login thresholds were properly implemented for [REDACTED] devices.

Facts and Evidence pertaining to the PV:

Evidence:

[REDACTED]

Facts:

The audit team reviewed evidence provided for sampled cyber assets, request [REDACTED]. In this evidence, [REDACTED] made the following statement from [REDACTED]: "[...] no security alerts for the sampled assets on the sampled dates."

The audit team issued [REDACTED] requesting [REDACTED] to provide evidence of all alerts for the sampled devices since June 1, 2015 and if no alerts exist for the sampled devices to provide a list of alerts for all devices since June 1, 2015. [REDACTED] provided [REDACTED] that stated [REDACTED] is the tool used by [REDACTED] for automated alerting. While pulling evidence for this data request, it was discovered there were no alerts being generated for the sampled assets. On 11/11/2015, the support team identified a configuration issue that prevented alerts from being sent out. The support team is working to resolve the configuration issue. [REDACTED] has a pending self-report for failure to alert on assets being monitored by [REDACTED].

The audit team issued [REDACTED] requesting [REDACTED] to provide an indication of how many assets are affected for [REDACTED] and the date the issue started for the [REDACTED] issue described in [REDACTED]. [REDACTED] provided [REDACTED] that stated "Please reference excel spreadsheet [REDACTED] for the affected list. The issue began on 4/30/2015 and included [REDACTED] devices." [REDACTED] also provided [REDACTED] detailing the assets affected by the issue.

[REDACTED]

While on-site, [REDACTED] provided updated information regarding the issue [REDACTED]. The actual issue was identified as a lack of an alert for [REDACTED] unsuccessful login attempts followed by a successful login for a total of [REDACTED] devices. All other alerting was enabled and working. [REDACTED]

[REDACTED] is the Security Information and Event Management (SIEM) Tool used by [REDACTED] for automated log alerting. [REDACTED] is in the process of migrating assets from two [REDACTED] SIEMs to a single primary SIEM in [REDACTED] and assets are being migrated over a several month period (April – November 2105).

- On 11/11/2015, the support team identified a configuration issue that prevented alerts from being sent out for one rule ' [REDACTED] consecutive unsuccessful authentication attempts followed by a successful authentication within a [REDACTED]
- The two original SIEMs were still able to alert (and no events were triggered June 1 – November 11, which is not unusual), however the new primary SIEM could not alert had any events been triggered.
- The SIEM tool was using an internal group to email alerts. Other rules also used this group with no issue. The resolution was to point to [REDACTED] to generate a ticket and alert the team. All other alerting rules were also changed. This issue was corrected the same day.
- On 12/4/2015, a manual review was completed and determined that no alerts had been generated and missed, however if an alert had been generated during this time from the primary SIEM, we would not have received it.
- A sample alert [REDACTED] - [REDACTED] Followed by Successful Logon within [REDACTED]' is provided to show the issue was corrected on 11/11/2015.

The audit team finds a possible violation for CIP-007-3 R6 (R6.2). The root cause is defined as a configuration issue for [REDACTED] alerting that resulted in no ability to issue alerts for unsuccessful login attempts (5) followed by a successful login for [REDACTED] devices beginning April 30, 2015. The issue was discovered November 11, 2015. Note that the audit is for CIP-007-5 R4 (Part 4.2) as part of the CIP Version 5 Transition Program.

Open Enforcement Actions:

[REDACTED]

[REDACTED]

For FFT Candidates ONLY

1. Why did this possible violation pose a minimal risk:
Only one particular type of alert was affected in the [REDACTED] configuration..
2. Has Registered Entity mitigated this possible violation: YES NO
 - a. If yes, describe mitigating actions and state the date that Registered Entity completed the mitigating actions:
Updated
[Click here to enter text.](#)
3. Please answer the following questions to determine whether this possible violation constitutes a “clear on its face” FFT candidate or a “close call.” If the answer to any of the following questions is yes, this possible violation will be treated as a “close call.” Otherwise, this possible violation will be treated as a “clear on its face” FFT candidate.
 - A. Is there any disagreement amongst the audit team on whether the PV is a “clear on its face” or “close call” candidate: YES NO
 - a. If yes, explain why:

[Click here to enter text.](#)
 - B. Does this possible violation reveal a serious shortcoming in registered entity’s reliability-related processes (e.g. a systematic compliance program failure):

YES NO
 - a. If yes, explain why:

[Click here to enter text.](#)
 - C. Are there any additional facts the audit team needs to know in order to comfortably designate this possible violation for FFT treatment: YES NO
 - a. If yes, state those facts:

[Click here to enter text.](#)
4. Did audit team inform registered entity that this possible violation qualifies for FFT treatment? YES NO
 - a. If so, on what date? [Enter Date.](#)

Attachment 33

Record documents for the violation of CIP-007-3a R7

33.a The Companies' Self-Report



This item was submitted by [REDACTED] on 8/11/2016

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: CIP-007-3a

Applicable Requirement: R7.

Applicable Sub Requirement(s): R7.1.

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: 3/10/2016

Beginning Date of Possible Violation: 3/10/2016

End or Expected End Date of Possible Violation: 7/30/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED] (CIP-007-3a, R7.1.)
 Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

As a result of equipment failures and/or replacements, two failed NERC CIP BCAs [REDACTED] were removed from the CIP Physical Security Perimeter (PSP) without following the sanitization and chain of custody processes established under [REDACTED] and the CIP standards.

One of these devices was located at [REDACTED] and one was located at [REDACTED]. The issues were discovered February 29 and March 24 2016, respectively.

[REDACTED]

Preliminary Causal Factors:
 [REDACTED] was not notified that the additional [REDACTED] were within NERC CIP scope. Additionally, there were a lack of process and rigor in regards to decommissioning practices within [REDACTED].

Although a formal cause analysis will be performed [REDACTED] believes the issue is likely an awareness and training matter within [REDACTED].

According to the Extent Of Condition responses received from other Business units, there are no other similar violations.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

Violation involving [REDACTED]

Violation involving [REDACTED]

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

In Addition:

- [REDACTED] discussed this issue in a weekly safety/staff meeting on Monday 3/14
- Direction from [REDACTED] includes initial details on responsibilities of [REDACTED] including:
 - o Additional devices being added as Cyber Assets.
 - o Steps to take for device sanitization
 - o Steps to take for chain of custody for device removal.

[REDACTED] developed device commissioning training and is delivering this training to technicians and supervisors in [REDACTED]

Provide details to prevent recurrence:

Process to be implemented:

- [REDACTED] plans to deliver training to other regions in the [REDACTED] footprint to help prevent recurrence.
- [REDACTED] will engage with the business areas to ensure greater awareness of the CIP standards and participate in the development and delivery of training

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

8/30/2016

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:

The Potential Impact to the Bulk Power System is minimal because of the following:

[REDACTED]

In Addition:

- [REDACTED] discussed this issue in a weekly safety/staff meeting on Monday 3/14
- Direction from [REDACTED] includes initial details on responsibilities of [REDACTED] including:
 - o Additional devices being added as Cyber Assets.
 - o Steps to take for device sanitization
 - o Steps to take for chain of custody for device removal.

[REDACTED] developed device commissioning training and is delivering this training to technicians and supervisors in [REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

[REDACTED] internal compliance plan was in effect at the time of the potential noncompliance, however, the communication to the proper parties that these two sites were brought into scope under CIP V3 was not adequate to prevent this violation.

The following steps will be implemented to prevent a re-occurrence of this event:

- [REDACTED] plans to deliver training to other regions in the [REDACTED] footprint to help prevent recurrence.
- [REDACTED] will engage with the business areas to ensure greater awareness of the CIP standards and participate in the development and delivery of training
- Provide Training to other [REDACTED] that may not have received [REDACTED] specific training.
- [REDACTED] needs greater involvement in this training

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.)

Attachment 34

Record documents for the violation of CIP-007-3a R8

34.a The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 9/2/2016

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: CIP-007-3a

Applicable Requirement: R8.

Applicable Sub Requirement(s): R8.4.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

4/30/2016

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: 1/6/2016

Beginning Date of Possible Violation: 11/17/2015

End or Expected End Date of Possible Violation: 8/8/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED] Regarding CVAs, CIP-007-3 R8.4 requires: Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

On 1/6/2016, during Internal Controls Assessment (ICA) testing, it was discovered that 1 Cyber Vulnerability (CVA) Action Plan had not been provided for a CVA that was completed on November 17, 2015. This was for [REDACTED] devices located at the [REDACTED]

A formal CVA Action Plan was not created or thought necessary by the [REDACTED] support team since the items identified in the CVA results are handled through on-going procedures and not in a CVA finding.

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

If Yes, Provide description of Mitigating Activities:

- On 3/23/2016, a CVA was performed to validate all items had been corrected by on-going procedures and no security flags were identified.
- Training on the current process for CVA Action Plans has been completed.
- A CVA Action Plan, documenting action items found during the November 2015 CVA, was formally documented on 3/9/2016.
- Support, in conjunction with support, will review the CVA Action Plan processes to identify any gaps between the respective processes, including identifying roles and responsibilities for developing and managing the CVA Action Plan

Provide details to prevent recurrence:

Persons responsible for creating and tracking the CVA Action Plans have received training on the current process and the related procedures.

For "end of life" assets being managed at the Support has a process for developing a CVA Action Plan to manage identified items. Support is in the process of reviewing their plan to ensure it covers all scenarios.

New devices being installed at the will be managed by the group. has a documented process for developing a CVA Action Plan to manage identified items.

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

3/9/2016

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:

The Potential Impact to the Bulk Power System is minimal. Action items documented in the CVA Action Plan required no non-routine work to resolve. In addition, the devices are located within an ESP and firewall rules associated with these devices are highly restricted, reducing the likelihood of unauthorized access to the devices.

Provide detailed description of Actual Risk to Bulk Power System:

There was no actual impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

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.)

Attachment 35

Record documents for the violation of CIP-007-3a R9

35.a The Companies' Self-Report



This item was submitted by [REDACTED] on 10/17/2017

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.2.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

[REDACTED]

Monitoring Method for previously reported or discovered:

On-site Audit

Has the scope of the Possible Violation expanded:

Yes

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

Date Possible Violation was discovered: 6/8/2017

Beginning Date of Possible Violation: 6/8/2017

End or Expected End Date of Possible Violation: 6/8/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-002-5.1 R1 [REDACTED] is obligated to implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

R1.1 is not applicable for this SR as it applies to high impact systems.

R1.2 requires [REDACTED] to identify each of the Medium Impact BES Cyber Systems according to Attachment 1, Section 2, if any at each asset.

R1.3 requires [REDACTED] to identify each asset that contains a low impact BES Cyber System according to Attachment 1 Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

[REDACTED] documented processes and Procedures applicable to this issue under CIP-002-5.1:

[REDACTED] processes to identify Medium Impact BES Cyber Systems is contained in [REDACTED] Cyber Asset Inventory Procedure and [REDACTED] Asset Identification & Classification (AIC) Identification of Cyber Assets Enterprise Procedure.

The [REDACTED] Cyber Asset Inventory Procedure [REDACTED] requires a physical walk-down of the facility to inventory all cyber assets.

[REDACTED] is used to perform the inventory [REDACTED] Cyber Asset Inventory Procedure.

grouped into BES Cyber Systems. [REDACTED] requires the Responsible Entity to create a list of BES Cyber Assets to be

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Applicable Sections of the documented processes:

Summary

During an subsequent inventory being performed for compliance with CIP-002-5.1 R2 on 6/08/17, [REDACTED] discovered a modem at [REDACTED] that should have been disconnected from a medium impact BES Cyber Asset and working phone line. The result was a possible violation of NERC CIP-002-5.1 R1.2 as the modem was not identified as part of the medium BES Cyber System it was attached to.

During the initial inventory performed for NERC CIP V5 implementation on 1/7/15, a modem is identified attached to a [REDACTED]. When the [REDACTED] is replaced on 4/6/16, the modem is left in place and connected to the new [REDACTED].

The cause of the modem being connected to the [REDACTED] was determined to be that NERC CIP Version 5 program processes had not been effectively implemented in the last quarter of 2015 when the project team designed the changes to replace the two [REDACTED] and that that during the design stage, the consultant did not recognize the need to remove the modem.

Timeline

[REDACTED]

Causes of the violation

Apparent Cause #1 Unawareness of Regulatory Implications

The [REDACTED] NERC CIP Version 5 program was in its early stages of development and processes had not been effectively implemented in the last quarter of 2015 when the project team designed the changes to replace the two [REDACTED]. The project team was not made aware of the possible NERC CIP violation associated with the modem being connected to the [REDACTED]. Therefore, the [REDACTED] did not consciously make the decision to disconnect the modem.

Apparent Cause #2 Unawareness- Inattention to Detail

[REDACTED]

During the extent of condition review in [REDACTED] other possible violations have been entered in with the same extent of condition.

[REDACTED]

[REDACTED]

[REDACTED]

The extent of condition did not identify any issues in [REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken include the following:

1. Implement the [REDACTED] NERC CIP Project Impact Checklist in [REDACTED]

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include the following:

[REDACTED]

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

12/15/2017

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:

The Potential Impact to the Bulk Electric System could have been moderate if the modem were able to communicate with the BES Cyber System.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because. Additionally, there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this potential violation.

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.)

Attachment 36

Record documents for the violation of CIP-009-6 R1

36a. The Companies' Self-Report



36b. The Companies' Self-Report



This item was submitted by [REDACTED] on 4/7/2017

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: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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: 1/5/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 1/11/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

The devices [REDACTED] reside in the [REDACTED] BCS and the following number of devices are with this BCS:

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Yes, these devices were reclassified as follows:

- a. Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- b. Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- c. Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide details to prevent recurrence:

A cause analysis will be performed to evaluate additional causal factors to identify effective corrective actions to prevent reoccurrence.

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

1/11/2017

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:

[REDACTED]

[REDACTED] there was minimal likelihood that the failure to identify these devices as EACMS resulted in unauthorized or unauthenticated activity that could adversely affect the Bulk Power System.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

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.)

This item was submitted by [REDACTED] on 1/23/2018

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

4/7/2017

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: Yes

If yes, indicate which Region(s):

[REDACTED]

Date Reported to Region(s):

4/7/2017

Date Possible Violation was discovered: 11/15/2017

Beginning Date of Possible Violation: 11/15/2017

End or Expected End Date of Possible Violation: 11/17/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP002-5, R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

Per sub-requirement R1.1:

Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

Problem Statement

[REDACTED] were not properly classified as High Impact Electronic Access Control or Monitoring Systems (EACMS), causing the devices to potentially not have full North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), resulting in this possible violation.

Additional Information:

Categorization of Bulk Electric System (BES) Cyber Assets (CAs), BCAs, is the process whereby [REDACTED] a CA and then assigns the appropriate categorization to that device. Proper categorization of EACMS ensures appropriate NERC CIP protections are implemented on the identified asset. PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

[REDACTED]

Method of Discovery

Self-Assessment: [REDACTED]

[REDACTED]

Extent Of Condition:

As part of the [REDACTED] the [REDACTED] group will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all [REDACTED] will need to 1) reassess their technologies to ensure alignment with the [REDACTED] and 2) ensure [REDACTED] Level processes support the new program which may require the [REDACTED] to work through the asset classification process for all assets under the revised program.

Cause Analysis:

This violation occurred as a result of:

- Lack of specificity within the [REDACTED] requirements of the process, no process available.

Cause Identification:

- Prior self-reported issues with [REDACTED] and other firewall rules focused on systems designed to facilitate IRA were incorrectly implemented due to the lack of clarity in the [REDACTED] program
- [REDACTED] [REDACTED] and [REDACTED] were not properly assessed in the V5 transition as being Intermediate Systems
- [REDACTED] [REDACTED] and [REDACTED] were not previously identified as EACMS because their primary function was not to enable remote access

The direct and contributing causes of this possible violation:

Apparent Cause 1 (AC1): Process Weakness. Lack of specificity within the [REDACTED] requirements of the process; no process available.

Prior self-reported issues with [REDACTED] and other firewall rules, focused on systems designed to facilitate IRA and were incorrectly implemented due to the lack of clarity during the implementation of the [REDACTED] program.

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

[i](#) An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Actions [REDACTED] has already completed to remediate this potential violation include:

On 11/28/2017, [REDACTED] determined this violation a self-report and the [REDACTED] team submitted the appropriate [REDACTED] ticket workflow to correctly update the categorization and create the necessary work orders to apply the appropriate controls to the identified devices.

Completed: As of 12/4/2017, all identified devices have been re-categorized as EACMS.

Provide details to prevent recurrence:

██████████ has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that ██████████ will incur further risk of the same or similar NERC reliability standard violation.

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE. THIS INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

See section 7.0 Corrective Actions (Fixes) Recommended by Cause Analysis Team for respective milestone dates.

- CIP-002 ██████████ ██████████ to provide updated CIP-002 ██████████ documentation that will be used by all ██████████ to perform a gap analysis and re-evaluation of in-scope BES Cyber Assets
- With oversight from ██████████ all ██████████ to perform a business procedure / gap analysis between the current CIP-002 / ██████████ business procedures and the updated CIP-002 / ██████████ documentation
- With oversight from ██████████ all ██████████ to provide a draft of CIP-002 / ██████████ business level procedures
- With oversight from ██████████ all ██████████ to obtain ██████████ business level procedures approved
- With oversight from ██████████ all ██████████ to identify those individuals who require training on updated CIP-002 / ██████████ business level procedures
- With oversight from ██████████ all ██████████ to communicate and provide training on updated CIP-002 / ██████████ business level procedures to those individuals requiring training
- With oversight from ██████████ all ██████████ to re-evaluate / re-classify BES Cyber Assets based on updated business level procedures and submit potential violation if identified
- ██████████ to submit ██████████ tickets to initiate workflow necessary to re-classify identified devices as EACMS
- ██████████ to perform an active review of All ██████████ Management Systems to determine if any additional systems have been improperly classified
- ██████████ to submit ██████████ tickets to push firewall rules for scanning identified devices
- ██████████ to perform security controls testing (SCT) on identified devices

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

11/28/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

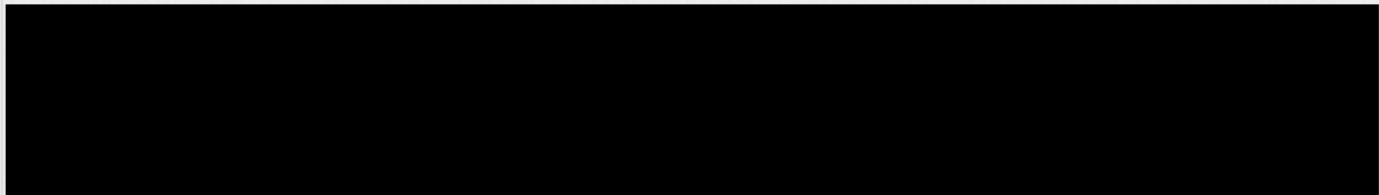
Baseline management including:

- 1) Operating system/firmware
- 2) Software version
- 3) Logical network accessible ports
- 4) Security patches
- 5) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

██████████ did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

The likelihood that this event would adversely impact the Bulk Electric System is considered minimal because:



Additional Comments:

This violation was not the result of intentional action to violate a NERC reliability standard. ██████████ was attempting to comply in good faith with the applicable NERC reliability standard at issue in this potential violation. The ██████████ internal compliance plan was in effect at the time of the potential noncompliance. ██████████ management relevant to the situation actively participated and encouraged employees to provide complete information.

There have been no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance.

Attachment 37

Record documents for the violation of CIP-009-6 R2

37.a The Companies' Self-Report [REDACTED]

37.b The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 1/23/2018

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

4/7/2017

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: Yes

If yes, indicate which Region(s):

[REDACTED]

Date Reported to Region(s):

4/7/2017

Date Possible Violation was discovered: 11/15/2017

Beginning Date of Possible Violation: 11/15/2017

End or Expected End Date of Possible Violation: 11/17/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP002-5, R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

Per sub-requirement R1.1:

Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

Problem Statement

[REDACTED] were not properly classified as High Impact Electronic Access Control or Monitoring Systems (EACMS), causing the devices to potentially not have full North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), resulting in this possible violation.

Additional Information:

Categorization of Bulk Electric System (BES) Cyber Assets (CAs), BCAs, is the process whereby a CA and then assigns the appropriate categorization to that device. Proper categorization of EACMS ensures appropriate NERC CIP protections are implemented on the identified asset. PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

[Redacted]

Method of Discovery

Self-Assessment: [Redacted]

[Redacted]

Extent Of Condition:

As part of the [Redacted] the [Redacted] will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all [Redacted] will need to 1) reassess their technologies to ensure alignment with the [Redacted] and 2) ensure [Redacted] Level processes support the new program which may require the [Redacted] to work through the asset classification process for all assets under the revised program.

Cause Analysis:

This violation occurred as a result of:

- Lack of specificity within [Redacted] requirements of the process, no process available.

Cause Identification:

- Prior self-reported issues with [Redacted] focused on systems designed to facilitate IRA were incorrectly implemented due to the lack of clarity in the [Redacted]
- [Redacted] were not properly assessed in the V5 transition as being Intermediate Systems
- [Redacted] were not previously identified as EACMS because their primary function was not to enable remote access

The direct and contributing causes of this possible violation:

Apparent Cause 1 (AC1): Process Weakness. Lack of specificity within [Redacted] requirements of the process; no process available.

Prior self-reported issues with [Redacted] focused on systems designed to facilitate IRA and were incorrectly implemented due to the lack of clarity during the implementation of the [Redacted]

[Redacted]

Are Mitigating Activities in progress or completed? Yes

[An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.](#)

If Yes, Provide description of Mitigating Activities:

Actions [Redacted] has already completed to remediate this potential violation include:

On 11/28/2017, [Redacted] determined this violation a self-report and the [Redacted] submitted the appropriate [Redacted] workflow to correctly update the categorization and create the necessary work orders to apply the appropriate controls to the identified devices.

Completed: As of 12/4/2017, all identified devices have been re-categorized as EACMS.

Provide details to prevent recurrence:

has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that will incur further risk of the same or similar event. **PROTECTED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

See section 7.0 Corrective Actions (Fixes) Recommended by for respective milestone dates.

- CIP-002 IT503 Refresh to provide updated CIP-002 documentation that will be used by all to perform a gap analysis and re-evaluation of in-scope BES Cyber Assets
- With oversight from all to perform a business procedure / gap analysis between the current CIP-002 business procedures and the updated CIP-002 documentation
- With oversight from all to provide a draft of CIP-002 business level procedures
- With oversight from all to obtain business level procedures approved
- With oversight from all to identify those individuals who require training on updated CIP-002 business level procedures
- With oversight from all to communicate and provide training on updated CIP-002 business level procedures to those individuals requiring training
- With oversight from all to re-evaluate / re-classify BES Cyber Assets based on updated business level procedures and submit potential violation if identified
- to submit to initiate workflow necessary to re-classify identified devices as EACMS
- to perform an active review of All Management Systems to determine if any additional systems have been improperly classified
- to submit to push firewall rules for scanning identified devices
- to perform security controls testing (SCT) on identified devices

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

11/28/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

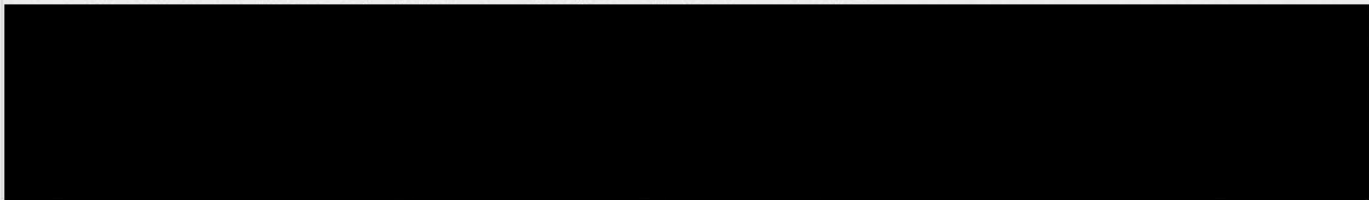
Baseline management including:

- 1) Operating system/firmware
- 2) Software version
- 3) Logical network accessible ports
- 4) Security patches
- 5) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

The likelihood that this event would adversely impact the Bulk Electric System is considered minimal because:



Additional Comments:

This violation was not the result of intentional action to violate a NERC reliability standard. was attempting to comply in good faith with the applicable NERC reliability standard at issue in this potential violation. The internal compliance plan was in effect at the time of the potential noncompliance. management relevant to the situation actively participated and encouraged employees to provide complete information.

There have been no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance.

This item was submitted by [REDACTED] on 4/7/2017

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: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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: 1/5/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 1/11/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

The devices [REDACTED] reside in the [REDACTED] and the following number of devices are with this BCS:

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Yes, these devices were reclassified as follows:

- a. [REDACTED] - 74357 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- b. [REDACTED] - 74363 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- c. [REDACTED] - 74355 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17

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

Provide details to prevent recurrence:

A cause analysis will be performed to evaluate additional causal factors to identify effective corrective actions to prevent reoccurrence.

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

1/11/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal [REDACTED]

Actual Impact to the Bulk Power System: Minimal [REDACTED]

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

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.)

Attachment 38

Record documents for the violation of CIP-009-6 R3

38a. The Companies' Self-Report [REDACTED]

38.b The Companies' Self-Report [REDACTED]

38.c The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 11/27/2017

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

4/7/2017

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: 8/1/2017

Beginning Date of Possible Violation: 5/5/2017

End or Expected End Date of Possible Violation: 8/8/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

During a meeting between a [REDACTED] and a [REDACTED] a concern was raised that BCA [REDACTED] was not categorized correctly in the [REDACTED] database. After further investigation it was determined that the associated server [REDACTED] was categorized correctly, however, the associated [REDACTED] was categorized as "No Tier".

August 8, 2017:

[REDACTED] ticket was submitted for the re-assessment of [REDACTED] and to apply the appropriate controls for a BES Cyber Asset.

Cause Analysis:

[REDACTED]

Extent Of Condition:

The extent of condition analysis for this potential violation originally focused on the [REDACTED] application used by [REDACTED] to manage NERC CIP assets. [REDACTED] does not use any other asset management tool, such as [REDACTED], to manage NERC CIP assets, where this condition might occur.

A further extent of condition was performed for all other applicable business units to determine if the potential for an asset classification violation could exist in their respective area.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Conclusion:

[REDACTED]

[REDACTED] has previously reported this violation and corrective actions were completed. See [REDACTED]

[REDACTED]

[REDACTED] - The annual Cyber Vulnerability Assessment review concluded that devices had incorrect NERC CIP Classification assigned. See [REDACTED]

[REDACTED] - Has identified several cases where devices were incorrectly classified as Medium when they should have been classified as Low. This "administrative" error did not result in a potential violation.

[REDACTED]

No CIP002-5 R1 issues identified.

[REDACTED] Support:

This support group is no longer performing asset classification. All new assets that support [REDACTED] are being managed by the [REDACTED] organization and follow [REDACTED] asset classification processes.

No CIP002-5 R1 issues identified.

[REDACTED]

Both support groups collaborate with [REDACTED] lead to verify the location and function of the device being categorized. Through this collaboration the proper categorization is determined.

No CIP002-5 R1 issues identified.

Associated Asset: [REDACTED]

BES Cyber System: [REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System:

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

Baseline management including:

- 3) Operating system/firmware
- 4) Software version
- 5) Logical network accessible ports
- 6) Security patches
- 7) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

[REDACTED] did not identify any actual impact to the Bulk Electric System as a result of this potential violation.

[REDACTED] considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

[REDACTED]

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.)

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [REDACTED] on 11/27/2017

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

4/7/2017

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: 8/1/2017

Beginning Date of Possible Violation: 5/5/2017

End or Expected End Date of Possible Violation: 8/8/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

[REDACTED]

August 8, 2017:

[REDACTED] ticket was submitted for the re-assessment of [REDACTED] and to apply the appropriate controls for a BES Cyber Asset.

Cause Analysis:

[REDACTED]

Extent Of Condition:

The extent of condition analysis for this potential violation originally focused on the [REDACTED] application used by [REDACTED] to manage NERC CIP assets. [REDACTED] does not use any other asset management tool, such as [REDACTED] to manage NERC CIP assets, where this condition might occur.

A further extent of condition was performed for all other applicable business units to determine if the potential for an asset classification violation could exist in their respective area.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Conclusion:

[REDACTED]

[REDACTED] has previously reported this violation and corrective actions were completed. See [REDACTED]

[REDACTED]

[REDACTED] - The annual Cyber Vulnerability Assessment review concluded that devices had incorrect NERC CIP Classification assigned.

See [REDACTED]

[REDACTED] - Has identified several cases where devices were incorrectly classified as Medium when they should have been classified as Low. This "administrative" error did not result in a potential violation.

[REDACTED]

No CIP002-5 R1 issues identified.

[REDACTED]

Support:
This support group is no longer performing asset classification. All new assets that support [REDACTED] are being managed by the [REDACTED] organization and follow [REDACTED] asset classification processes.

No CIP002-5 R1 issues identified.

[REDACTED]

Both support groups collaborate with [REDACTED] lead to verify the location and function of the device being categorized. Through this collaboration the proper categorization is determined.

No CIP002-5 R1 issues identified.

[REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System:

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

Baseline management including:

- 3) Operating system/firmware
- 4) Software version
- 5) Logical network accessible ports
- 6) Security patches
- 7) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

[REDACTED] did not identify any actual impact to the Bulk Electric System as a result of this potential violation.

[REDACTED] considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

[REDACTED]

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 I, Section 6.4.)

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

This item was submitted by [REDACTED] on 1/23/2018

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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): [REDACTED]

Date Reported to Region or Discovered by Region: [REDACTED]

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: Yes

If yes, indicate which Region(s): [REDACTED]

Date Reported to Region(s): 4/7/2017

Date Possible Violation was discovered: 11/15/2017

Beginning Date of Possible Violation: 11/15/2017

End or Expected End Date of Possible Violation: 11/17/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP002-5, R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

Per sub-requirement R1.1:
Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

Problem Statement

[REDACTED] were not properly classified as High Impact Electronic Access Control or Monitoring Systems (EACMS), causing the devices to potentially not have full North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), resulting in this possible violation.

Additional Information:

Categorization of Bulk Electric System (BES) Cyber Assets (CAs), BCAs, is the process whereby a CA and then assigns the appropriate categorization to that device. Proper categorization of EACMS ensures appropriate NERC CIP protections are implemented on the identified asset. PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

[Redacted]

Method of Discovery

Self-Assessment: [Redacted]

[Redacted]

Extent Of Condition:

As part of the [Redacted] the [Redacted] will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all [Redacted] will need to 1) reassess their technologies to ensure alignment with the [Redacted] and 2) ensure [Redacted] processes support the new program which may require the [Redacted] to work through the asset classification process for all assets under the revised program.

Cause Analysis:

This violation occurred as a result of:

- Lack of specificity within the [Redacted] requirements of the process, no process available.

Cause Identification:

- Prior self-reported issues with [Redacted] focused on systems designed to facilitate [Redacted] were incorrectly implemented due to the lack of clarity in the [Redacted]
- [Redacted] were not properly assessed in the V5 transition as being Intermediate Systems
- [Redacted] were not previously identified as EACMS because [Redacted]


The direct and contributing causes of this possible violation:

Apparent Cause 1 (AC1): Process Weakness. Lack of specificity within the [Redacted] requirements of the process; no process available.

Prior self-reported issues with [Redacted] focused on systems designed to facilitate [Redacted] and were incorrectly implemented due to the lack of clarity during the implementation of the [Redacted]

[Redacted]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Actions [Redacted] has already completed to remediate this potential violation include:

On 11/28/2017, [Redacted] determined this violation a self-report and the [Redacted] submitted the appropriate [Redacted] workflow to correctly update the categorization and create the necessary work orders to apply the appropriate controls to the identified devices.

Completed: As of 12/4/2017, all identified devices have been re-categorized as EACMS.

Provide details to prevent recurrence:

██████████ has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that ██████████ will incur further risk of the same or similar NERC reliability standard violation.

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE. THIS DOCUMENT HAS BEEN REDACTED FROM THIS PUBLIC VERSION

See section 7.0 Corrective Actions (Fixes) Recommended by Cause Analysis Team for respective milestone dates.

- CIP-002 ██████████ Refresh. ██████████ to provide updated CIP-002 ██████████ documentation that will be used by all ██████████ to perform a gap analysis and re-evaluation of in-scope BES Cyber Assets
- With oversight from ██████████ all ██████████ to perform a business procedure / gap analysis between the current CIP-002 / ██████████ business procedures and the updated CIP-002 / ██████████ documentation
- With oversight from ██████████ all ██████████ to provide a draft of CIP-002 / ██████████ business level procedures
- With oversight from ██████████ all ██████████ to obtain ██████████ business level procedures approved
- With oversight from ██████████ all ██████████ to identify those individuals who require training on updated CIP-002 / ██████████ business level procedures
- With oversight from ██████████ all ██████████ to communicate and provide training on updated CIP-002 / ██████████ business level procedures to those individuals requiring training
- With oversight from ██████████ all ██████████ to re-evaluate / re-classify BES Cyber Assets based on updated business level procedures and submit potential violation if identified
- ██████████ to submit ██████████ to initiate workflow necessary to re-classify identified devices as EACMS
- ██████████ to perform an active review of All ██████████ to determine if any additional systems have been improperly classified
- ██████████ to submit ██████████ to push firewall rules for scanning identified devices
- ██████████ to perform security controls testing (SCT) on identified devices

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

11/28/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

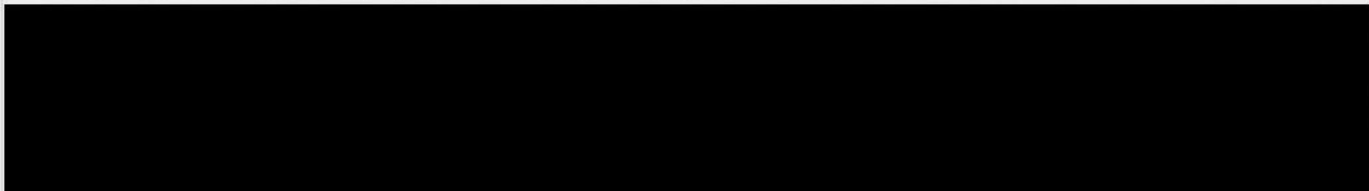
Baseline management including:

- 1) Operating system/firmware
- 2) Software version
- 3) Logical network accessible ports
- 4) Security patches
- 5) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

██████████ did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

The likelihood that this event would adversely impact the Bulk Electric System is considered minimal because:



Additional Comments:

This violation was not the result of intentional action to violate a NERC reliability standard. ██████████ was attempting to comply in good faith with the applicable NERC reliability standard at issue in this potential violation. The ██████████ internal compliance plan was in effect at the time of the potential noncompliance. ██████████ management relevant to the situation actively participated and encouraged employees to provide complete information.

There have been no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance.

Attachment 39

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

- 39a. Audit Summary [REDACTED]
- 39.b The Companies' Self-Report [REDACTED]
- 39.c The Companies' Self-Report [REDACTED]
- 39.d The Companies' Self-Report [REDACTED]
- 39.e Audit Summary [REDACTED]
- 39.f The Companies' Self-Report [REDACTED]
- 39.g The Companies' Self-Report [REDACTED]
- 39.h The Companies' Self-Report [REDACTED]
- 39.i The Companies' Self-Report [REDACTED]
- 39. j The Companies' Self-Report [REDACTED]
- 39.k Audit Summary [REDACTED]
- 39.l The Companies' Self-Report [REDACTED]
- 39.m The Companies' Self-Report [REDACTED]
- 39.n The Companies' Self-Report [REDACTED]
- 39.o The Companies' Self-Report [REDACTED]
- 39.p The Companies' Self-Report [REDACTED]

Post On-site Audit/Off-site Audit/Spot Check/Investigation Screening Worksheet

Prepared By: [REDACTED]

Submittal Date: [REDACTED]

Compliance Monitoring Method (On-site Audit, Off-site Audit, Spot-Check, or Investigation):
On-site Audit

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

Registered Entity Contact Information:

Name: [REDACTED]

Email: [REDACTED]

Standard: CIP-002-5.1

Requirement: R1

Sub Requirement(s): 1.2.4

Function(s) Applicable to Possible Violation:

[REDACTED]

Date violation occurred: 7/1/2016

Date violation discovered (Exit Presentation Date): [REDACTED]

Is the violation still occurring? Yes No

Are mitigating activities (including details to prevent reoccurrence) in progress or completed? Yes No

If yes, Provide description of Mitigating Activities:

Date Mitigating Activities are expected to be completed or were completed:

[REDACTED]

Detailed explanation and cause of violation: [REDACTED] Cyber Assets at th [REDACTED]
[REDACTED] were decommissioned in [REDACTED], yet appeared in the [REDACTED]
spreadsheet as provided to the auditors. Auditors noted these still appeared on the [REDACTED]
(master Cyber Asset inventory list) as it was provided on [REDACTED].

Potential Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

Actual Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

Detailed description of Potential Risk to Bulk Power System: The devices were decommissioned but left on the list. Since the devices were decommissioned there was no avenue for attack by an insider or outsider. This was a documentation error.

Detailed description of Actual Risk to Bulk Power System: This was a documentation error leaving devices on a list as opposed to deleting the assets from the list by leaving the assets in place. The assets were decommissioned so there was no ability to mount an attack through them.

Additional Comments: [REDACTED]
[REDACTED]
[REDACTED]

Auditors had inquired about these [REDACTED] devices during the physical walk-down. The numbers (last five digits of naming convention) listed correlates to the [REDACTED] (master Cyber Asset List) provided while on-site [REDACTED].

Please complete the form as completely as possible and email to [REDACTED]

This item was submitted by [REDACTED] on [REDACTED]

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: CIP-010-2
Applicable Requirement: R1.
Applicable Sub Requirement(s): 1.1.
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):

[REDACTED]

Date Reported to Region or Discovered by Region:

12/9/2016

Monitoring Method for previously reported or discovered:

On-site Audit

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: [REDACTED]

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 6/16/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]
In accordance with CIP-010-2 R1.1, [REDACTED] is required to implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 - Configuration Change Management. The Requirements for 1.1.1 specifically states [REDACTED] will develop a baseline configuration, individually or by group, which shall include Operating system(s) (including version) or firmware where no independent operating system exists. On 6/14/17, during execution of the annual Cyber Vulnerability Assessment (CVA), [REDACTED] discovered a discrepancy in the Firmware Version(s) listed in the System Security Baseline, thus [REDACTED] is in possible violation of CIP-010-2 R1.1.1 due to administrative change control deficiencies.
On [REDACTED] [REDACTED] compared screen prints of the Firmware Versions obtained from the Physical Access Control System (PACS) for each NERC CIP V5 [REDACTED] to the System Security Baseline.
During this review, [REDACTED] discovered the following errors:
1. Two (2) NERC CIP v5 [REDACTED] were listed on the System Security Baseline as having [REDACTED] installed, when in actuality, the screen print showed [REDACTED]. The two (2) [REDACTED] in question were: 1) [REDACTED] and 2) [REDACTED]. Note: [REDACTED] installed [REDACTED] for these sites prior to the NERC CIP V5 compliance date of 7/1/16; therefore, a System Security Baseline with respective Firmware Versions did not exist for validation.
2. The System Security Baseline did not list Firmware Version [REDACTED] as one of the current approved versions.
To perform the Extent of Condition of the [REDACTED] NERC CIP V5 [REDACTED] logged into the PACS, validated each [REDACTED] Firmware Version, and compared them to the System

Security Baseline. During this evaluation, [REDACTED] discovered additional administrative errors on the System Security Baseline as follows:

1. The screen prints for 14 [REDACTED] showed [REDACTED] installed, however the System Security Baseline showed [REDACTED].
2. The System Security Baseline did not include [REDACTED] on the list of approved systems.

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Errors discovered during the Extent of Condition analysis affecting [REDACTED] include:

[REDACTED]

[REDACTED] developed the System Security Baseline with information received from the [REDACTED] in August 2015. [REDACTED] approved the final version of the System Security Baseline on 6/29/16, prior to the 7/1/16 NERC CIP V5 compliance effective date. At the time of the approval, [REDACTED] did not perform a device-by-device validation and verification comparing the individual [REDACTED] to the System Security Baseline.

On Friday, 6/23/17, [REDACTED] received written confirmation from the vendor that there were no material or security differences in the three (3) Firmware Releases, therefore no Cyber vulnerabilities existed due to these discrepancies.

[REDACTED] initial cause analysis of this possible violation indicates deficiencies in administrative change control, process weaknesses, human performance, management oversight, and lack of validation and verification.

Nature and Number of Devices Involved

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] performed the following actions to correct the System Security Baseline:

- 1) [REDACTED] updated the Firmware Version for [REDACTED]
- 2) [REDACTED] updated the System Security Baseline to depict the correct Firmware Versions for all [REDACTED]
- 3) [REDACTED] added Firmware Version [REDACTED] to the [REDACTED] System Security Baseline.

[REDACTED] performed the following reconciliations of the System Security Baseline:

- 1) Compared the devices listed in the System Security Baseline to the [REDACTED] Asset Inventory Classification (AIC) list to ensure accuracy between the reports.
- 2) Conducted a review of the [REDACTED] Firmware Versions indicated in the PACS screenshots (dated 6/15/17 and 6/16/17) to ensure the version listed in the System Security Baseline was accurate.

Are Mitigating Activities in progress or completed? 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:

The Potential Impact to the Bulk Electric System is minimal because the discrepancy was due to administrative errors on the System Security Baseline and no security vulnerabilities existed. Upon discovery, [REDACTED] performed a review of the [REDACTED] Firmware Versions installed in the field and updated the System Security Baseline to match the installations for [REDACTED] sites. In addition, the Firmware Versions were reconciled and updated on the System Security Baseline.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Electric System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Electric System as a result of this alleged violation.

Additional Comments:

This potential violation was not the result of intentional action to violate a NERC reliability standard.

██████████ was attempting to comply in good faith with the applicable NERC reliability standard at issue in this potential violation.

██████████ management at all levels relevant to this situation actively participated and encouraged employees to provide complete information.

There were no extenuating circumstances with respect to the cause of the potential violation.

██████████ conducted a cross-functional Extent of Condition analysis, which included ██████████. Results are as follows:

- ██████████ discovered discrepancies on their System Security Baseline on 7/6/17 as part of the annual CVA. The errors occurred during the creation of the original baseline in 2016. A Self-Report is presently under development. ██████████ has implemented controls to prevent additional errors to their System Security Baseline.
- ██████████ conducted a review of their System Security Baseline and confirmed that similar conditions do not exist within their organization.
- ██████████ confirmed their organization does not have similar conditions for System Security Baseline Firmware discrepancies. However, the ██████████ auditors discovered a System Security Baseline discrepancy during the ██████████ in regards to ports and services. This potential violation is part of an audit finding ██████████. IT has implemented automated tools and procedural controls to prevent recurrence of errors to their System Security Baselines.

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.)

This item was submitted by [REDACTED] on 11/28/2017

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: CIP-010-2

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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: 7/1/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 4/16/2018

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to all Jurisdictions [REDACTED]

During the first annual performance of the Cyber Vulnerability Assessments, [REDACTED] discovered possible violations of a Reliability Standard Requirement. [REDACTED] discovered a number of inaccuracies with [REDACTED] These include BES Cyber Assets (BCAs) that are not in an [REDACTED] BCAs in the incorrect [REDACTED] BCAs with incorrect firmware documented and inconsistencies with documentation of enabled logical ports and services.

Reference to:
 CIP-010-2. Cyber Security-Configuration Change Management and Vulnerability Assessments, R1.1 -
 CIP-010-2, R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.
 R1.1. Develop a baseline configuration, individually or by group, which shall include the following items:
 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;
 1.1.2. Any commercially available or open-source application software (including version) intentionally installed;
 1.1.3. Any custom software installed;
 1.1.4. Any logical network accessible ports; and
 1.1.5. Any security patches applied.

Apparent Cause (AC1): Inadequate configuration and change control.
 Description: The failure to ensure CIP compliance evidence and documentation is collected and updated in a timely manner.

Apparent Cause (AC2): Lack of properly defined process or procedure.
 Description: The accurate completion of the [REDACTED] compliance inventory and the SSB are dependent upon human interaction with verification and validation check points. The lack of a process or procedure to outline the expectations allows for more human error to exist.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Severe

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The actions that [REDACTED] is taking to prevent recurrence include the following:
 1. [REDACTED] to complete CVA Possible Compliance Findings and provide documentation to validate completion of each

action in the plan. Complete 10/16/2017

2. [REDACTED] will validate completion of Possible Compliance Findings and verification by [REDACTED] Complete

10/31/2017

3. Document a process for the automated tool which validates [REDACTED] against [REDACTED] compliance inventory. Complete 10/27/2017

4. [REDACTED] to complete CVA Possible Compliance Findings (see appendix) and provide documentation to validate

completion of each action in the plan. Complete 10/27/2017

5. [REDACTED] will validate completion of Possible Compliance Findings and verification by [REDACTED] Complete

11/15/2017

6. [REDACTED] to complete CVA Possible Compliance Findings (see appendix) and provide documentation to

validate completion of each action in the plan. Complete 11/30/2017

7. [REDACTED] implementation:

Implement consistent configuration and change control process across all jurisdictions to ensure accurate and timely [REDACTED] and

updates are made. Due Date: 12/1/2017

8. [REDACTED] will validate completion of Possible Compliance Findings and verification by [REDACTED] Due DATE:

12/15/2017

9. Using the automated tool and the process developed in CA#3, perform an initial audit/validation of [REDACTED] against the [REDACTED]

compliance inventory. Adjust the automated tool as necessary. Due Date: 12/15/2017

10. Identify specific individual(s) in each region to ensure [REDACTED] inventory and baseline accuracy. Due Date: 01/15/2018

11. [REDACTED] to complete CVA Possible Compliance Findings (see appendix) and provide documentation to

validate completion of each action in the plan. Due Date: 1/31/2018

12. [REDACTED] will validate completion of Possible Compliance Findings and verification by [REDACTED] Due Date:

02/14/2018

13. [REDACTED] to complete CVA Possible Compliance Findings (see appendix) and provide documentation to validate

completion of each action ue Date: 03/30/2018

14. [REDACTED] will validate completion of Possible Compliance Findings and verification by [REDACTED] Due Date:

04/16/2018

Provide detailed description of Actual Risk to Bulk Power System:

The purpose of documenting and maintaining accurate [REDACTED] on an ongoing basis is to ensure appropriate awareness of the existing security characteristics for BES Cyber Assets in order to ensure any changes to the systems do not negatively impact the security controls protecting the devices. With inaccuracies in the baselines and unauthorized changes being made to the systems, the security characteristics of the devices are not completely known and therefore the security controls applied to the devices may not be adequate. As a result, the potential impact to the Bulk Electric System (BES) could be serious if an adversary were successful in gaining access to the devices (physical and/or electronic) and in identifying and exploiting deficiencies or gaps in the security controls.

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.)

This item was submitted by [REDACTED] on [REDACTED]

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: CIP-007-6

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

8/4/2016

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: [REDACTED]

Beginning Date of Possible Violation: 8/1/2016

End or Expected End Date of Possible Violation: 8/26/2016

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED]
On [REDACTED] during the review of sampled baseline documents during the [REDACTED] device baselines did not match device configurations for open ports and services. The devices were [REDACTED] EACMS and [REDACTED]

The ephemeral ports above [REDACTED] were omitted from the baseline in error.

Device identified during initial review:

[REDACTED]

As a result of this discovery, [REDACTED] device documentation, for medium impact stations, has been checked for ephemeral port ranges and updated.

Devices identified during further investigation of baseline documentation as compared to configuration data:

[REDACTED]

Based on the 'Extent of Condition' conducted among [REDACTED] functions, the [REDACTED] function has experienced identical procedural errors. When processing a CVA, ports and services discrepancies were sited. Further investigation is required to determine the number of devices with this discrepancy.

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

The mitigating activities underway are to review and correct the baselines for the affected devices. As a result of this discovery, [REDACTED] device documentation, for medium impact stations, has been checked for ephemeral port ranges and updated. Further mitigating activities are to review each [REDACTED] device configuration comparing the data to the documented baseline ports and services.

Provide details to prevent recurrence:

Details related to preventing the recurrence of this human error are to be identified during development of mitigation plan and cause analysis.

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

8/26/2016

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:

The potential impact to the Bulk Power System is minimal because the devices have the required CIP protections. In addition, the devices are secured behind a firewall and enclosed in a physically secured perimeter, both monitored 24/7, and requiring account and password access.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there was no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of the alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

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.)

**Post On-site Audit/Off-site Audit/Spot Check/Investigation Screening
Worksheet**

Prepared By: [REDACTED]

Submittal Date: [REDACTED]

Compliance Monitoring Method (On-site Audit, Off-site Audit, Spot-Check, or Investigation):
On-Site Audit

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

Registered Entity Contact Information:

Name: [REDACTED]

Email: [REDACTED]

Standard: CIP-010-2

Requirement: R1

Sub Requirement(s): R1.1

Function(s) Applicable to Possible Violation:

[REDACTED]

Date violation occurred: 07/01/2016

Date violation discovered (Exit Presentation Date): [REDACTED]

Is the violation still occurring? Yes No

Are mitigating activities (including details to prevent reoccurrence) in progress or completed? Yes No

If yes, Provide description of Mitigating Activities:

Date Mitigating Activities are expected to be completed or were completed:

[REDACTED]

Detailed explanation and cause of violation: While on-site, the audit team discovered that [REDACTED] failed to develop a baseline configuration, individually or by group, which shall include the following items:

1.1.4. Any logical network accessible ports;

[REDACTED] For device [REDACTED], auditors noticed that baseline DID NOT contain ALL ports and services thus resulting in a possible violation of CIP-010 R1.1.4. This possible violation is in conjunction with CIP-007-6 R1.1.

Potential Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

Actual Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

Detailed description of Potential Risk to Bulk Power System: The potential impact to the Bulk Power System is minimal because the devices have the required CIP protections. In addition, the devices are secured behind a firewall and enclosed in a physically secured perimeter, both monitored 24/7, and requiring account and password access.

Detailed description of Actual Risk to Bulk Power System: There was Minimal Impact to the Bulk Power System caused by this possible violation. This determination is due to the fact that no actual event or adverse consequences occurred.

Additional Comments:

Note: Cyber Assets, [REDACTED] and [REDACTED] are physically ONE device but logically seperated with independent IP addresses.

[REDACTED] Responses to data request, show evidence entity developed baseline configurations for an auditor-selected sample of Cyber Assets, effective as of an auditor-selected date (July 10, 2016).

[REDACTED] [REDACTED]) and associated files listed within document.

Please complete the form as completely as possible and email to [REDACTED]

This item was submitted by [REDACTED] on 10/9/2017

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: CIP-007-3a

Applicable Requirement: R2.

Applicable Sub Requirement(s): R2.1.

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: 6/28/2017

Beginning Date of Possible Violation: 6/30/2016

End or Expected End Date of Possible Violation: 12/31/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

In June 2017, during the [REDACTED] review and Cyber Vulnerability Assessments for [REDACTED] it was discovered that the [REDACTED] Within [REDACTED] the device 'running configuration' is used to document ports and services. The 'running configuration' documents the ports and services based on a point in time; it does not document the entire range of potential open ports.

The system used to control [REDACTED] assets, [REDACTED] is a [REDACTED] product. Based upon the version of the [REDACTED] various dynamic port ranges are used. With the majority of the [REDACTED] devices having an operating system of [REDACTED]

The [REDACTED] system communicates using two internet protocols [REDACTED] and [REDACTED]. The communication path [REDACTED] and [REDACTED] elicit dynamic port ranges from the [REDACTED]. The baseline which was performed in 2016 per procedure [REDACTED] did not include the most current [REDACTED] dynamic port range, [REDACTED] used under both protocols.

During the performance of 2016 annual cyber vulnerability assessment, discussions between [REDACTED] and [REDACTED] identified that the range was smaller than documented in the [REDACTED] Operations Manual due to the majority of the [REDACTED] being [REDACTED]. [REDACTED] documented the minimum port range based on historical scans. Though there was discussion in 2016 regarding the use of a smaller port range, the issue was not escalated to the correct level to ensure ongoing compliance.

[REDACTED]

The Baseline was updated to include the missing ports in order to correct the noncompliance per CIP-007 R1, R1.1, CIP-010 R1.1.4. Peer validation was completed following the update.

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

The following mitigating activities were performed:

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

- 1. Update baseline documents to include the appropriate [redacted] based on the vendor manual for the [redacted]
- 2. Conducted a review of baseline documents to determine if this situation existed in other [redacted]
- 3. Reviewed the [redacted] baseline procedure to ensure use of vendor documented ports used when creating baseline documents.
- 4. Conducted an [redacted] Extent of Condition to identify other business areas with [redacted]

Provide details to prevent recurrence:

In order to prevent recurrence, the [redacted] baseline procedure has been updated and appropriate compliance personnel trained on the updated procedure.

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

8/18/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal [redacted]

Actual Impact to the Bulk Power System: Minimal [redacted]

Provide detailed description of Potential Risk to Bulk Power System:

[Redacted]

Provide detailed description of Actual Risk to Bulk Power System:

[Redacted]

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.)

This item was submitted by [REDACTED] on 3/29/2017

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: CIP-010-2

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.3.

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: 8/23/2016

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 7/26/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

Per CIP-010-2 R1 Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-2 R1. CIP-010-2 R1.3 states for a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

On 06/20/2016, [REDACTED] entered [REDACTED] ticket [REDACTED] as a placeholder to document the transition of compliance activities/responsibilities for the [REDACTED] appliance from [REDACTED] to [REDACTED]. [REDACTED] after taking ownership of the [REDACTED] applied [REDACTED] as an upgrade to the [REDACTED]. [REDACTED] The change was made using existing [REDACTED] change management processes and tools as shown in [REDACTED] however, the change management processes and tool had not been updated to address NERC CIP requirements. As a result the required baseline was not performed and the baseline artifact was not updated within the required amount of time.

After [REDACTED] learned of the missing baseline for the [REDACTED] an updated baseline was created by [REDACTED] to reflect the current state of the device on 07/26/2016, which was past the 30 calendar days permitted by the standard.

The following are the identified assets:

[REDACTED]

The number of assets are as follows:

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

If Yes, Provide description of Mitigating Activities:

To mitigate missing NERC CIP processes for the [redacted] group the following activities have been implemented:
[redacted] support staff received guidance for updating baseline evidence from [redacted]. [redacted] was the group who had transferred ownership to [redacted].
(Status: Completed, Date:07/26/2016)
*Increased qualified personnel expanding workforce flexibility.
(Status: Completed, Date:12/31/2016)

Provide details to prevent recurrence:

To ensure corrective action effectiveness, sustainability and to prevent reoccurrence a cause analysis will be performed to evaluate additional casual factors and corrective actions.

In addition, the cause analysis will specifically look to determine if:
*Processes for transferring Cyber Assets between [redacted] business units.
*Review mitigation activities shown above to ensure the activities have all the required processes and evidence artifacts required to maintain NERC CIP compliance.

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

7/26/2016

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:

The potential impact to the Bulk Power System for placing a Cyber Asset into service without a current baseline could have been unneeded ports, services, software and users which may have been exploited to compromise the Cyber Asset.

Another impact to the Bulk Power System could be security and risk decisions regarding the [redacted] appliance were made with stale data and could have been erroneous.

There was minimal potential impact to the Bulk Power System because the [redacted]

Provide detailed description of Actual Risk to Bulk Power System:

There was minimal Actual Impact to the Bulk Power System caused by this possible violation because of the following:
*The [redacted] appliance was updated to the latest approved vendor operating system image.
*No critical issues were identified as part of the [redacted] baseline update performed by [redacted] (On 07/26/2016, the [redacted] and the supporting [redacted] was updated by [redacted] to reflect the current state of the device).
[redacted] system logs were reviewed for the time period of the possible violation and no inappropriate access or activities were identified.
Additional Comments Instructions

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[redacted] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

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.)

This item was submitted by [REDACTED] on 2/2/2017

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: CIP-010-2

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.2.

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: 9/1/2016

Beginning Date of Possible Violation: 8/31/2016

End or Expected End Date of Possible Violation: 9/1/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On 8/31/2016 at about 4:30 PM the [REDACTED] was installed on [REDACTED] devices at the [REDACTED]. The planned install was pushed by the [REDACTED] management console without a change control ticket being submitted.

A [REDACTED] change control ticket ([REDACTED] is a work management system) should have been submitted prior to the change taking place so that all of the proper controls were performed prior to the installs. The individual who performed this change neglected to follow procedure and create the appropriate change control ticket as needed. Instead, the individual performed this change outside of the designated procedure.

On 9/14/2016, [REDACTED] ticket [REDACTED] was submitted in support of the installation of the [REDACTED] agent on these devices. Security Controls Testing was performed and completed via Security Control Test # [REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? 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:

There is minimal impact to the Bulk Power System because all prior installs have occurred without any known issues. This software was intended to be installed on these devices. However, the potential impact to the Bulk Electric System would be that due to this change being made, there could have been an unexpected error or issue that occurred during the install process that could possibly propose a security risk, that otherwise may have been discovered and mitigated if the correct change control process was followed. Compromise would be unlikely or risk would have been limited due to the NERC CIP requirements and protections in place, including being located within the PSP (Physical Security Perimeter, and in an ESP (Electronic Security Perimeter).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

An Extent of Condition was completed on 9/15/16 for [REDACTED] There were no issues identified that were related to this condition.

[REDACTED] has a similar violation which was reported to [REDACTED] as [REDACTED]

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation. The [REDACTED] internal compliance plan that was in effect at the time of the potential noncompliance. [REDACTED] management relevant to the situation actively participated and encouraged employees to provide complete information.

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.)

This item was submitted by [REDACTED] on 3/7/2017

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: CIP-010-2

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.2.

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):

[REDACTED]

Date Reported to Region or Discovered by Region:

2/2/2017

Monitoring Method for previously reported or discovered:

Self-Certification

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: 2/6/2017

Beginning Date of Possible Violation: 2/2/2017

End or Expected End Date of Possible Violation: 2/3/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

The assets were patched without a change ticket to support the upgrade. This occurred because the [REDACTED] Analyst did not perform a verification to determine if a change ticket existed, believing that the patches were already covered under an existing patch cycle / and corresponding change ticket.

On 2/2/2017, a [REDACTED] Analyst applied [REDACTED] patches to two (2) EACMs prior to submitting a [REDACTED] Change Control ticket.

As part of routine operations, [REDACTED] Analyst verifies changes applied to a BES cyber asset have a corresponding [REDACTED] change ticket.

On 2/3/2017, during the routine review performed by a [REDACTED] Analyst, it was determined that the change identified in the [REDACTED] asset did not have an associated change ticket. Once it was determined that a change ticket had not been submitted to support the installation of the [REDACTED] patches, the [REDACTED] analyst initiated the Potential Violation Self Report (PVSR) process by contacting [REDACTED] and a full investigation was initiated.

The following EACMs have been identified in this potential violation:

[REDACTED]

Assets in the Associated BES Cyber Systems

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Yes, after the issue was identified on 2/3/2017 [REDACTED] change tickets [REDACTED] was entered by the [REDACTED] Analyst to account for these changes.

Provide details to prevent recurrence:

A cause analysis will take place to assist in preventing recurrence of this possible violation.

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

2/3/2017

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:

Testing was performed on the patches and vetted and accepted prior to being installed which determined that the patches posed no threat to the bulk power system.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this potential violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this potential violation.

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.)

This item was submitted by [REDACTED] on 1/12/2018

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: CIP-010-2

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.2.

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): [REDACTED]

Date Reported to Region or Discovered by Region:

3/7/2017

Monitoring Method for previously reported or discovered:

Self-Certification

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: 10/31/2017

Beginning Date of Possible Violation: 10/27/2017

End or Expected End Date of Possible Violation: 10/31/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

CIP 010-2 R1.2: Authorize and document changes that deviate from the existing baseline configuration.

During the [REDACTED] daily [REDACTED] review on 10/30/2017, it was noted that [REDACTED] software had been installed on [REDACTED] workstations located at the [REDACTED]. The installation occurred on 10/27/2017. It was discovered that the installation happened without an associated change request ticket (CRQ). All [REDACTED] workstations are defined as high BES cyber assets (BCAs). The analyst that reviewed the [REDACTED] report contacted the engineer who performed the change request; the engineer stated that he thought that CRQ-1251 was entered and approved by his manager for the [REDACTED] software installation. Upon further investigation, it was determined that CRQ-1251 had a primary change window start date of 10/31/2017. The analyst created one (1) CRQ to cover the first [REDACTED] assets, and overlooked creating the 2nd CRQ to cover the last [REDACTED] workstations. The actual change occurred four days ahead of the documented scheduled primary change window start date. The change also occurred prior to CRQ-1251 being approved by [REDACTED] and the Change Management Coordinator (CMC).

In summary, a software installation occurred ahead of the scheduled time frame documented in CRQ-1251. Also, CRQ-1251 did not get the final approvals from [REDACTED] and CMC necessary to complete the CRQ approval process until 10/31/2017.

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

- A CRQ was created and approved for installing [REDACTED] software to the [REDACTED] BCAs.
- Performed a mandatory stand-down/in-person meeting with the [REDACTED] support team, communicating the recent possible violation (PV) and the requirements associated with performing BCA changes.
- Forwarded a summary of the [REDACTED] support team business area stand-down call, regarding BES Cyber Asset changes, to all [REDACTED] support team business area managers with a requirement to review with their respective teams.
- Modified the final change control approval email notification to include all devices approved on a CRQ.

Provide details to prevent recurrence:

Successful completion of the mitigation plan will prevent or minimize the probability that [REDACTED] will incur further risk of the same or similar NERC requirements in the future.

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

12/12/2017

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:

The potential impact to the Bulk Power System is minimal as the [REDACTED] BCA workstations had been identified to receive the software update. However, the nine workstations were overlooked during the ticket creation process. These [REDACTED] workstations were similar to others that were successfully updated with an appropriate CRQ. The updates did not cause a security risk and the baselines were updated upon approval of the CRQ, thus maintaining the risk as minimal.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

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.)

Post On-site Audit/Off-site Audit/Spot Check/Investigation Screening Worksheet

Prepared By: [REDACTED]

Submittal Date: [REDACTED]

Compliance Monitoring Method (On-site Audit, Off-site Audit, Spot-Check, or Investigation):
On-Site Audit

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

Registered Entity Contact Information:

Name: [REDACTED]
Email: [REDACTED]

Standard: CIP-010-2

Requirement: R1

Sub Requirement(s): R1.4

Function(s) Applicable to Possible Violation:

[REDACTED]

Date violation occurred: 07/01/2016

Date violation discovered (Exit Presentation Date): [REDACTED]

Is the violation still occurring? Yes No

Are mitigating activities (including details to prevent reoccurrence) in progress or completed? Yes No

If yes, Provide description of Mitigating Activities:

Date Mitigating Activities are expected to be completed or were completed:

[REDACTED]

Detailed explanation and cause of violation: While on-site, the audit team discovered that [REDACTED] failed to: 1.4.1. determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;
1.4.2. verify that required cyber security controls determined in 1.4.1 are not adversely affected; and
1.4.3. document the results of the verification.

[REDACTED] Auditor selected cyber asset [REDACTED] was changed from the then existing baseline when the firmware was upgraded to another version. A System Security Baseline also existed for this new firmware and the device was moved to the appropriate System Security baseline. No documentation for determination, verification, or results of the required cyber security controls in CIP-005 and CIP-007 are available for the change to [REDACTED] [REDACTED], resulting in a possible violation of R1.4.

Potential Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

Actual Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

Detailed description of Potential Risk to Bulk Power System: The potential impact to the Bulk Power System is minimal because the devices have the required CIP protections. In addition, the devices are secured behind a firewall and enclosed in a physically secured perimeter, both monitored 24/7, and requiring account and password access.

Detailed description of Actual Risk to Bulk Power System: There was Minimal Impact to the Bulk Power System caused by this possible violation. This determination is due to the fact that no actual event or adverse consequences occurred.

Additional Comments: Reference Information: [REDACTED]
[REDACTED]

Please complete the form as completely as possible and email to [REDACTED]

This item was submitted by [REDACTED] on 12/18/2017

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: CIP-010-2

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.4.

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: 9/12/2017

Beginning Date of Possible Violation: 7/12/2017

End or Expected End Date of Possible Violation: 9/22/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED]
9/11/2017 – During reviews of change management testing scans, a [REDACTED] analyst noticed that IDPS Security Controls Test (Security Controls Test) scans were unavailable for two (2) devices [REDACTED]. The [REDACTED] analyst notified the [REDACTED] team that the scans were not available. The [REDACTED] team verified they did not have SCT scans in their scanning tool for either [REDACTED] IDPS.

9/12/2017 – A review of all BES CSI [REDACTED] was conducted in an effort to locate SCT scans produced, but not listed in the scanning tool. No SCT scans were found.

After an investigation, it was determined that human error occurred as the [REDACTED] devices were listed in the change ticket but left off of the SCT scan job that was performed on 7/12/2017 thus resulting in a possible violation of NERC CIP 10-2 R1.4.

Cause Analysis:

The cause analysis was performed to determine whether the incident revolved around an equipment failure, process weakness or human performance. While gathering facts and investigating the incident, it was determined that the incident occurred due to a lack of a procedure. The facts of the incident assisted with identifying human performance and organizational challenges. The apparent cause was lack of management oversight due to lack of a procedure to handle work orders.

An Extent of Condition was requested of the business areas to perform checks for the appropriate documentation for a review of CIP-005 (firewall and interactive remote access) and CIP-007 (ports and services, etc.), before and after changes, to determine if there were deviations from the existing baseline configuration. The business areas reviewed their manual baseline changes (number of changes reviewed=10) or automatic baseline changes (number of changes reviewed=50) and did not identify any missing documentation based on the review of CIP-005 and CIP-007 before and after changes.

BES Cyber System Information:

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

In order to mitigate the possible violation, the SCT scans were performed on the two (2) IPDS devices.

Provide details to prevent recurrence:

Successful completion of the mitigation plan will prevent or minimize the probability that [REDACTED] will incur further risk of the same or similar NERC requirements in the future:

- Create a procedure to verify work order requirements are met.
- Communicate applicable personnel on the procedure to handle work order expectations.
- Train [REDACTED] team on the procedure to handle work order expectations.
- Add training to verify work order requirements to on-boarding activities for new or transferring employees added to the [REDACTED] team.
- Create a requirements/best practices document on work order requests and completion for business areas.
- Create a "best practices" document on work order requests and completion for business areas.
- Communicate the "best practices" document to respective business areas.
- Collaborate with key business areas to build a procedure to review scans within the same timeframe the scan was produced in order to confirm whether changes have occurred in baseline configurations and address any actions that need to be processed.
- Collaborate with those business areas to communicate the procedure to review scans to key personnel for awareness to determine if changes have occurred in baseline configurations.

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

10/13/2017

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:

The potential impact to the Bulk Power System is minimal as the protections that are in place via the firewall rules prevent unauthorized protocol from traversing the network. The IDPS devices were not compromised by not having the SCT scans performed and functionality continued as normal. After the scans were performed, it was confirmed that there were no cyber security controls adversely affected.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

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.)

This item was submitted by [REDACTED] on 8/31/2016

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: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.2.

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: 7/20/2016

End or Expected End Date of Possible Violation: 7/20/2016

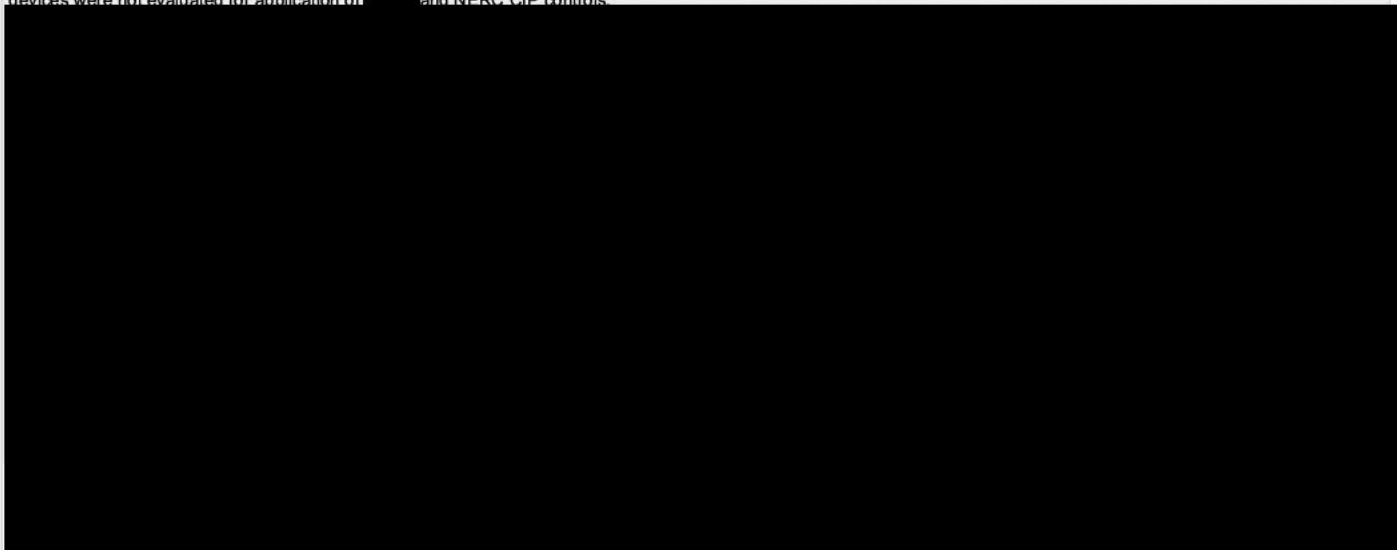
Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP-002-5.1 R1.2., [REDACTED] is obligated to identify and classify Medium Impact Electronic Access Control and Monitoring Systems (EACMS).

During a review of the asset list, it was discovered that a [REDACTED] device was not labeled as and EACMS as expected. As a result, the devices were not evaluated for application of [REDACTED] and NERC CIP controls.



Are Mitigating Activities in progress or completed? Yes

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

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

If Yes, Provide description of Mitigating Activities:

[Redacted] has reviewed the SEIM classification and is in the process of performing a walk down at each station to reapply the internal policy for classifying an EACMS

Provide details to prevent recurrence:

Actions to prevent recurrence will be developed as part of the mitigation plan.

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

11/18/2016

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:

[Redacted]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

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.)

This item was submitted by [REDACTED] on 4/7/2017

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: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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: 1/5/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 1/11/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Yes, these devices were reclassified as follows:

- a. [REDACTED] - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- b. [REDACTED] - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- c. [REDACTED] - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17

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

Provide details to prevent recurrence:

A cause analysis will be performed to evaluate additional causal factors to identify effective corrective actions to prevent reoccurrence.

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

1/11/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal [REDACTED]

Actual Impact to the Bulk Power System: Minimal [REDACTED]

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

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.)

This item was submitted by [REDACTED] on 1/23/2018

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: CIP-002-5.1a

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

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): [REDACTED]

Date Reported to Region or Discovered by Region: 4/7/2017

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: Yes

If yes, indicate which Region(s): [REDACTED]

Date Reported to Region(s): 4/7/2017

Date Possible Violation was discovered: 11/15/2017

Beginning Date of Possible Violation: 11/15/2017

End or Expected End Date of Possible Violation: 11/17/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP002-5, R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

Per sub-requirement R1.1:
Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

Problem Statement

[REDACTED] were not properly classified as High Impact Electronic Access Control or Monitoring Systems (EACMS), causing the devices to potentially not have full North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), resulting in this possible violation.

Additional Information:

Categorization of Bulk Electric System (BES) Cyber Assets (CAs), BCAs, is the process whereby

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Method of Discovery

Self-Assessment:

Extent Of Condition:

As part of the [redacted] the [redacted] will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all [redacted] will need to 1) reassess their technologies to ensure alignment with the [redacted] and 2) ensure [redacted] processes support the new program which may require the [redacted] to work through the asset classification process for all assets under the revised program.

Cause Analysis:

This violation occurred as a result of:

- Lack of specificity within the [redacted] requirements of the process, no process available.

Cause Identification:


- Prior self-reported issues with [redacted] focused on systems designed to facilitate IRA were incorrectly implemented due to the lack of clarity in the [redacted]
- [redacted] were not properly assessed in the V5 transition as being Intermediate Systems
- [redacted] were not previously identified as EACMS because their primary function was not to enable remote access

The direct and contributing causes of this possible violation:

Apparent Cause 1 (AC1): Process Weakness. Lack of specificity within the [redacted] requirements of the process; no process available.

Prior self-reported issues with [redacted] focused on systems designed to facilitate IRA and were incorrectly implemented due to the lack of clarity during the implementation of the [redacted]

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitigating Activities:

Actions [redacted] has already completed to remediate this potential violation include:

On 11/28/2017, [redacted] determined this violation a self-report and the [redacted] submitted the appropriate [redacted] to correctly update the categorization and create the necessary work orders to apply the appropriate controls to the identified devices.

Completed: As of 12/4/2017, all identified devices have been re-categorized as EACMS.

Provide details to prevent recurrence:

has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that will incur further risk of the same or similar event.

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE. THIS INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

See section 7.0 Corrective Actions (Fixes) Recommended by Cause Analysis Team for respective milestone dates.

- CIP-002 Refresh. to provide updated CIP-002 documentation that will be used by all to perform a gap analysis and re-evaluation of in-scope BES Cyber Assets
- With oversight from all to perform a business procedure / gap analysis between the current CIP-002 / business procedures and the updated CIP-002 / documentation
- With oversight from all to provide a draft of CIP-002 / business level procedures
- With oversight from all to obtain business level procedures approved
- With oversight from all to identify those individuals who require training on updated CIP-002 / business level procedures
- With oversight from all to communicate and provide training on updated CIP-002 / business level procedures to those individuals requiring training
- With oversight from all to re-evaluate / re-classify BES Cyber Assets based on updated business level procedures and submit potential violation if identified
- to submit to initiate workflow necessary to re-classify identified devices as EACMS
- to perform an active review of All to determine if any additional systems have been improperly classified
- to submit to push firewall rules for scanning identified devices
- to perform security controls testing (SCT) on identified devices

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

11/28/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

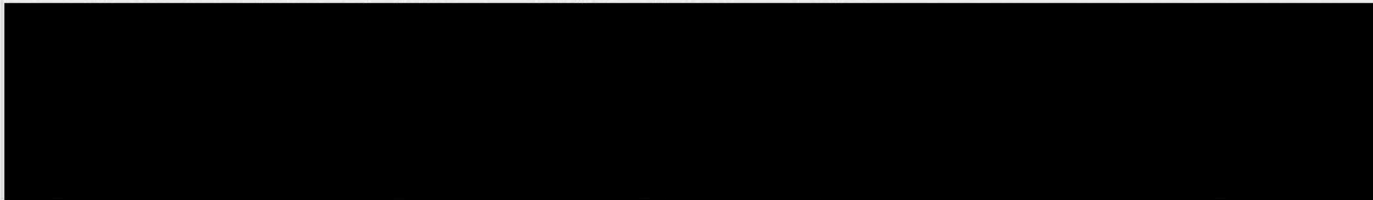
Baseline management including:

- 1) Operating system/firmware
- 2) Software version
- 3) Logical network accessible ports
- 4) Security patches
- 5) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

The likelihood that this event would adversely impact the Bulk Electric System is considered minimal because:



Additional Comments:

This violation was not the result of intentional action to violate a NERC reliability standard. was attempting to comply in good faith with the applicable NERC reliability standard at issue in this potential violation. The internal compliance plan was in effect at the time of the potential noncompliance. management relevant to the situation actively participated and encouraged employees to provide complete information.

There have been no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance.

