

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, [REDACTED]

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:

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.

Conclusion:

PRIVILEGED AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

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

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

See

- 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.

No CIP002-5 R1 issues identified.

Support:

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

No CIP002-5 R1 issues identified.

Both support groups collaborate with 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:

BES Cyber System:

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:

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

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

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 IV, Section 6.4.)

PRIVILEGED AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

## Attachment 40

Record documents for the violation of CIP-010-2 R2

40a. Audit Summary

40.b The Companies' Self-Report

40.c The Companies' Self-Report

40.d The Companies' Self-Report

40.e The Companies' Self-Report

40.f The Companies' Self-Report



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

Prepared By:

Submittal Date:

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

Registered Entity:

NERC Registry ID:

Registered Entity Contact Information:

Name:

Email:

Standard: CIP-010-2

Requirement: R2

Sub Requirement(s): R2.1

Function(s) Applicable to Possible Violation:

Date violation occurred: 07/01/2016

Date violation discovered (Exit Presentation Date):

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 Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.

Auditors noted that the August 2016 review of sampled cyber asset [REDACTED] was unavailable thus resulting in a possible violation.

Sampled cyber asset [REDACTED] for a High Impact BES Cyber System was put in production July 8, 2016 but logs were NOT reviewed within 35 calendar days as required thus resulting in a possible violation.

First review of changes to the baseline configuration occurred on September 8, 2016.

A total of [REDACTED] devices were 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: There was 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:

---

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

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: R2.

Applicable Sub Requirement(s): 2.1.

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:

8/31/2016

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: 2/22/2017

Beginning Date of Possible Violation: 7/11/2016

End or Expected End Date of Possible Violation: 2/26/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]


On 2/13/17, two analysts were performing a routine 35-day review for unauthorized changes. While reviewing the firewall [REDACTED] it was discovered that compliance scan tasks had not been executed for the time period of Dec 2016 and Jan 2017, approximately 87 days.

The firewall [REDACTED] is scanned every 35 days to ensure unauthorized changes have not occurred. [REDACTED]

There was no process in place to ensure the quality or accuracy of the CIP firewall list. Because of this [REDACTED] was not scanned and the required 35 day review was not performed to check for unauthorized changes.

The asset [REDACTED] and the following number of assets 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, a process is now in place to verify the CIP firewall list. The process consists of an analyst manually verifying the list and a second analyst performing a peer review of the CIP firewall list for accuracy. This process was executed on 2/23/2017 and is evidenced by a peer reviewed CIP firewall list and an associated verification report. This process will remain in place until the 3rd quarter 2017 when a full process redesign is introduced through the Configuration Management and Vulnerability Assessment project.

Provide details to prevent recurrence:

A Cause analysis will take place to assist in preventing recurrence of this possible violation. In addition, a full process redesign is underway with the Configuration Management and Vulnerability Assessment project which is slated for 3rd quarter 2017 completion.

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

2/23/2017

#### 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 a missing 35 day review scan does not impair firewall operability. The device was still operational and managed by the controlling firewall console. Subsequent scans showed no change to the system baseline during the missed period. Additionally, all security measures provided by the firewall remained in place and the device was providing traffic arbitration as expected. Had the device stopped operating an alert would be generated in the and support engaged to investigate.

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 because 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 [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: [REDACTED]

CIP-010-2

Applicable Requirement: [REDACTED]

R2.

Applicable Sub Requirement(s): [REDACTED]

2.1.

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]

3/29/2017

Monitoring Method for previously reported or discovered: [REDACTED]

Self-Report

Has the scope of the Possible Violation expanded: [REDACTED]

No

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

Date Possible Violation was discovered: [REDACTED]

Beginning Date of Possible Violation: 8/26/2016

End or Expected End Date of Possible Violation: 9/23/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:


This applies to [REDACTED]

Per CIP-010-2 R2 Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring R2.1 High Impact BES Cyber Systems and their associated Electronic Access Control and Monitoring Systems (EACMS). Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.

While preparing for the [REDACTED] Audit it was discovered [REDACTED] failed to monitor at least once every 35 calendar days for baseline configuration changes. [REDACTED] Audit preparation identified baseline configuration change monitoring due on 08/26/2016 was completed by [REDACTED] on 09/23/2016 missing the 35 day requirement.

The delay in baseline configuration change monitoring impacted [REDACTED] EACMS [REDACTED] located across [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:

To mitigate missing NERC CIP processes for the [REDACTED] the following activities have been implemented:  
\*Baseline configuration change review and monitoring artifacts put into evidence. (Status: Completed, Date: 09/23/2016)  
\* [REDACTED] members have added reoccurring 30 day task reminders to personal calendars. (Status: Completed, Date: 10/03/2016)  
\*Increased qualified personnel expanding workforce flexibility.  
(Status: Completed, Date: 12/31/2016)

Provide details to prevent recurrence:

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:

12/31/2016

#### 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 the [REDACTED] runs [REDACTED] only the required ports, services and users are active.

Provide detailed description of Actual Risk to Bulk Power System:

The Actual Impact to the Bulk Power System is minimal because of the following:



\*The [REDACTED] was updated to the latest approved vendor operating system image.

\*No critical issues were identified as part of the 09/23/2017 [REDACTED] baseline change monitoring update performed by [REDACTED].

\*[REDACTED] were reviewed for the time period of the possible violation and no inappropriate access or activities were identified.

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

**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 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: R2.

Applicable Sub Requirement(s): 2.1.

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: 9/12/2017

Beginning Date of Possible Violation: 8/12/2017

End or Expected End Date of Possible Violation: 9/14/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED]. On 9/11/2017, during reviews of change management testing scans, a [REDACTED] noticed two (2) IDPS [REDACTED] testing scans were unavailable. The [REDACTED] notified the [REDACTED] that the scans were not available. After a review by the [REDACTED] an issue was detected between the testing scanner [REDACTED] and both IDPS devices, therefore testing results were not returned when the scanner attempted to test both IDPS devices.

9/12/2017 – The [REDACTED] performed a review of prior 35-Day Unauthorized Change Reviews (UCR) which revealed two (2) missed 35-day cycles for IDPS devices due to the technological failure. The [REDACTED] SME reviewed the unauthorized change reports for the [REDACTED] devices and identified them as the same two (2) devices that missed the security control testing scan on 7/12/2017. On September 21, 2017, the [REDACTED] was submitted to repair the [REDACTED] communication issue. On September 30, 2017, the [REDACTED] was able to execute and return successful scans from the IDPS devices. A determination could not be made as to the reasoning for the communication error. However, the missed 35-day unauthorized change reviews resulted in a possible violation of NERC CIP 10-2 R2.1.


Cause Analysis:

During a review of CIP-010-2 R1.4 on September 11, 2017, two IDPS (Intrusion Detection/Intrusion Prevention) units were found to have a possible violation of NERC Standard CIP-010-2 R1.4 and CIP-010-2 R2.1. IDPS units monitor network traffic for malicious content. These IDPS units were in possible violation of CIP-010-2 R2.1 stemming from our inability to provide documentation or evidence of monitoring every 35 days for changes to the baseline. The cause analysis was performed to determine whether the incident revolved around an equipment failure, process weakness or human performance.

An Extent of Condition was performed by the business areas to review the last two (35- day) cycles for unauthorized changes that were missed or not documented properly. The business areas did not find any unauthorized changes that were missed or not documented accurately.

RES Cyber System Information: [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:

A scan was performed for 35-day unauthorized changes of the two IDPS devices that were previously not scanned.

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:

- The Cyber Security SMEs will review the [REDACTED] configuration scans. The dashboards will no longer be used.
- Develop operational 35-day UCR procedure with step-by-step instructions.
- Communicate operational 35-day UCR procedure with step-by-step instructions.
- 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 confirm if changes have occurred in baseline configurations.

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

10/2/2017

#### 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 with the firewall rules prevent malicious communication from traversing through the network. The IDPS devices were not compromised by not having the SCT scans performed and functionality continued as normal. Once the scans were performed, this confirmed that the system did not have any 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 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:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

## REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.1.

Applicable Functions:

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:

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

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]

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] 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] 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] 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] 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 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 / 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.

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



## Attachment 41

Record documents for the violation of CIP-010-2 R3

41.a The Companies' Self-Report dated [REDACTED]

41.b Audit Summary [REDACTED]

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

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

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

41.f 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-010-2

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: 7/15/2016

Beginning Date of Possible Violation: 7/14/2016

End or Expected End Date of Possible Violation: 12/31/2016

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED]. On July 15, 2016, while [REDACTED] SME was reviewing an automated [REDACTED] anomaly report, it was determined that a NERC CIP asset [REDACTED] had been moved from the "build" non production network to the production ESP network without following the proper change control procedures.

After further investigation, it was determined the NERC CIP asset [REDACTED] which was in a "Pre Production" status, had [REDACTED] that needed to be completed as part of the commissioning process prior to moving the asset on to the production ESP network, however the SME failed to complete the tickets and follow the correct commissioning process.

Because the SME installing the device failed to follow the commissioning process, an active vulnerability assessment was not performed on the asset prior to putting the asset into production. The failure not to have completed an active vulnerability assessment prior to placing the Cyber Asset into production violates CIP 010 2 R3.3.

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 mitigating activities that [REDACTED] has taken with respect to this issue include the following:  
- Proper commissioning activities including a vulnerability assessment was performed.

Provide details to prevent recurrence:

A detailed Cause Analysis investigation will take place over the next several weeks with the objective being to identify other potential mitigating controls to prevent future



reoccurrences.

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:

12/30/2016

#### MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Project Plan	9/30/2016	Project Plan Development	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:

Potential risk to the Bulk Power System is minimal because although a CVA was not completed for this asset, antivirus is installed as part of the standard build which was performed in a physical security perimeter by NERC trained technicians.

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.

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.)



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

---

Prepared By:

Submittal Date:

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

---

Registered Entity:

NERC Registry ID:

Registered Entity Contact Information:

Standard: CIP-010-2

Requirement: R3

Sub Requirement(s): R3.3

Function(s) Applicable to Possible Violation:

Date violation occurred:

Date violation discovered (Exit Presentation Date):

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 adhere to CIP-010-2 R3 Part 3.3: Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.

[REDACTED] Cyber Assets for a High Impact BES Cyber System was put in production without having an active pre-production vulnerability assessment.

**Sampled cyber assets:**

[REDACTED]  
[REDACTED]  
[REDACTED]  
[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 risk to the Bulk Power System is minimal because although a CVA was not completed for these assets; other controls were observed to be in place. Antivirus is installed as part of the standard device build, performed in a physical security perimeter by NERC CIP trained technicians.

**Detailed description of Actual 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 following time interval

**Additional Comments:**

[REDACTED]

---

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

This item was submitted by [REDACTED] on 1/23/2017

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: R3.

Applicable Sub Requirement(s): 3.3.

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:

7/15/2016

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: 9/22/2016

Beginning Date of Possible Violation: 9/16/2016

End or Expected End Date of Possible Violation: 9/23/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

On September 22, 2016, while a [REDACTED] SME was reviewing an automated [REDACTED] it was determined that (1) NERC CIP asset had been moved from [REDACTED] network to the production ESP network prior to performing a Cyber Vulnerability Assessment (CVA).

On 9/16/2016, [REDACTED] was updated per standard processes to show that the CIP asset moved from "pre-production" to "production."

On 9/22/2016, while reviewing the [REDACTED] it was discovered that the asset was not in compliance with the malicious software prevention and did not have the AV client installed. Due to this discovery, a [REDACTED] and indicated that the asset was not in compliance with the malicious software prevention and did not have the AV client installed.

On 9/26/2016, [REDACTED] ticket [REDACTED] was entered into [REDACTED] to decommission and retire the asset, [REDACTED] A new asset was configured appropriately and commissioned. The decision to commission a new asset was made to help expedite the process of getting an appropriately configured asset in place in lieu of the extra time it would take to configure [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:

The potential risk to the Bulk Power System was moderate because a cyber vulnerability assessment (CVA) was not performed and the device did not have virus protection installed; therefore there was the potential for the device to be compromised; however, the device was not compromised and is afforded NERC CIP protections that include being inside of an Electronic Security Perimeter (ESP) and a Physical Security Perimeter (PSP).

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. Although a CVA was not completed for this asset prior to being put into production, the issue was identified and corrected quickly. Additionally, the assets are afforded the protections of being inside an ESP and PSP.

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.)

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:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

## REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.2.

Applicable Functions:

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).

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:

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]

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

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]

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:

As a step in the build process for a net new server to support a net new instance of the , the conducted the categorization review of this new server. During this review on 11/15/2017, he consulted with the regarding the uses of this server. The

During the categorization review conducted between the and the

These devices were not previously identified as EACMS. Prior self-reported issues with and other

After more discussion with a

Extent Of Condition:

As part of the the will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all

Cause Analysis:

This violation occurred as a result of:

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

Cause Identification:

- Prior self-reported issues with and other firewall rules focused on systems designed to facilitate IRA were incorrectly implemented due to the lack of clarity in the
- were not properly assessed in the V5 transition as being Intermediate Systems
- 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 requirements of the process; no process available.

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 has already completed to remediate this potential violation include:

On 11/28/2017, determined this violation a self-report and the team submitted the appropriate 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. ██████████

PROVIDER 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 ██████████ 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 ██████████ 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

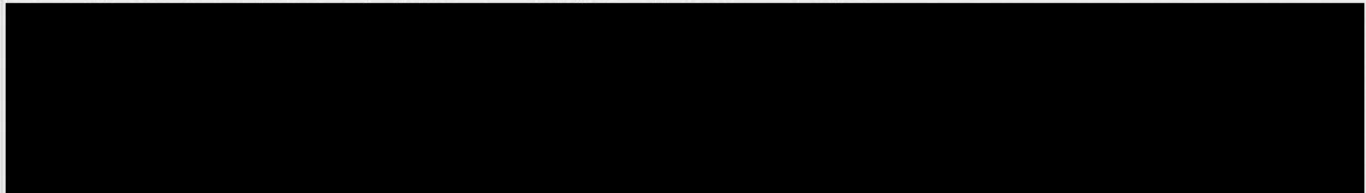
Baseline management including:

- 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





## Attachment 42

Record documents for the violation of CIP-010-2 R4

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

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

This item was submitted by [REDACTED] on 11/17/2017

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-010-2

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: No

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

Date Possible Violation was discovered: 5/30/2017

Beginning Date of Possible Violation: 5/30/2017

End or Expected End Date of Possible Violation: 5/28/2018

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This Self-Report covers [REDACTED]

Per CIP-010-2, Requirement 4 (R4), [REDACTED] shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCAs) and Removable Media that include the sections in Attachment 1. R4 is applicable to high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets. R4 contains Section 1 which is specific to TCAs managed by [REDACTED] and includes:

Section 1.1. - Transient Cyber Assets Management: Responsible entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

Section 1.2.1. - Transient Cyber Assets Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize: Users, either individually or by group or role.

Section 1.2.3. - Transient Cyber Assets Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize: Uses, which shall be limited to what is necessary to perform business functions.

Section 1.3. - Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability): (1) security patching, including manual or managed updates; (2) live operating system and software executable only from read-only media; (3) system hardening; or (4) other method(s) to mitigate software vulnerabilities.

Section 1.4 - Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability): (1) Antivirus software, including manual or managed updates of signatures or patterns; (2) Application whitelisting; or (3) Other method(s) to mitigate the introduction of malicious code.

Section 1.5 - Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s): (1) Restrict physical access; (2) Full-disk encryption with authentication; (3) Multi-factor authentication; or (4) Other method(s) to mitigate the risk of unauthorized use.

During an internal audit in May of 2017, the four Transient Cyber Asset (TCA) observations listed below were noted as possible violations, which under certain circumstances, could all lead to the same consequence: loss of situational awareness and/or control of Bulk Electric System (BES) components (e.g. loss of equipment, load, or generation).

1. TCAs used by Unauthorized Personnel: [REDACTED] sampled TCAs [REDACTED] were used by unauthorized personnel (i.e. users who were not authorized on the applicable business area's TCA Authorization Form). Business Areas are required to authorize individuals to use the TCAs and also ensure all users connecting TCAs to applicable systems have authorized electronic access to those systems. The TCA local users and users connecting TCAs to

applicable systems were authorized; however, remote users using [REDACTED] support tools [REDACTED] connect to TCAs were not authorized. The unauthorized users were IT support personnel with administrative rights who are [REDACTED] employees (undergone the standard [REDACTED] background checks). Unauthorized users having access to these TCAs could lead to theft of data or passwords from the TCA, or accidental or intentional misuse leading to malicious software being uploaded to the TCA. TCAs have antivirus protections in place to address malicious software; however, the potential [REDACTED] consequences and confidential information [REDACTED] HAS BEEN REDACTED FROM THIS PUBLIC VERSION [REDACTED] unavailability of the TCA and/or unavailability of the ESP network devices to which the TCA eventually connects.

2. TCAs with Unauthorized Software [REDACTED] - [REDACTED] sampled TCAs had software installed that was not on the applicable Business Area's TCA Software Authorization Form. Business Areas are required to approve all TCA software applications on their Business Area's TCA authorization form prior to installation. If the unauthorized software contains malicious code, this code could be passed to the Cyber Assets inside the ESP to which the TCA is connected, assuming the TCA antivirus protections in place to address malicious code do not prevent this.

3. TCAs absent from [REDACTED] - [REDACTED] sampled TCAs were absent from the [REDACTED] as of the end of May 2017. The [REDACTED] indicates which TCAs are on the corporate network to receive the required patching. To investigate further and determine the total number of TCAs absent from this report, [REDACTED] expanded the sample to the full TCA population. During this review of the full population, [REDACTED] determined [REDACTED] TCAs and [REDACTED] were absent from the [REDACTED] If TCAs did not receive security patches or antivirus updates, malicious code could be passed to the Cyber Assets inside the ESP to which the TCAs connect.

4. TCA Software Missing Patch Tracking Documentation [REDACTED] - [REDACTED] sampled TCAs had authorized Business Area specific software installed, but the related patch source was not being tracked in the Business Area level documentation. Business Areas are required to create and implement a TCA security patch management process for the patching of software that is not part of the corporate image. Any patches not being tracked may indicate the security patches are not being applied. If TCAs did not receive security patches and the TCA antivirus protections don't address malicious code, the TCA could pass malicious code to the Cyber Asset inside the ESP to which it connects.

The cause analysis and extent of condition (EOC) efforts indicated a lack of clear definition for the management of TCAs and control expectations for either ongoing and/or on-demand approaches.

Additionally, reviews of [REDACTED] also confirmed the lack of a clear position for managing TCAs. The current [REDACTED] guidance is that [REDACTED]

These facts lead to the inability to ensure ongoing compliance with TCA requirements.

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:

- The Potential Impact to the Bulk Power System is moderate because with access to the TCA, an individual with malicious intent would potentially be able to:
- Install malicious software to the TCA causing compromise to the TCA and/or compromise of the BCAs and PCAs to which the TCA eventually connects to serially,
  - Adversely affect situational awareness and/or control of Bulk Electric System components (e.g. loss of equipment, load, or generation).
- There was low likelihood that these events would adversely impact the Bulk Electric System for these reasons:
- Prior to connecting the TCA to a BCA and/or PCA, a user is required to have Physical Access to the applicable Physical Security Perimeters (PSPs).
  - Antivirus protections are in place to mitigate the introduction of malicious code.
  - [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.

[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 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:

R4.

Applicable Sub Requirement(s): [REDACTED]

Applicable Functions: [REDACTED]

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

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

Date Possible Violation was discovered: 7/26/2017

Beginning Date of Possible Violation: 7/26/2017

End or Expected End Date of Possible Violation: 7/26/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP-010-2 R4, [REDACTED] is obligated to implement for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.

CIP-010-2 Attachment 1 Section 1 Transient Cyber Asset(s) Managed by the Responsible Entity.  
Section 1.2 Requires [REDACTED] to authorize for each individual or group of Transient Cyber Asset(s):  
1.2.1. Users, either individually or by group or role;  
1.2.2. Locations, either individually or by group; and  
1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

[REDACTED] documented processes and Procedures applicable to this issue under CIP-010-2:

[REDACTED] process to manage TCAs is contained in [REDACTED]

[REDACTED] procedure to support the Enterprise process is contained in [REDACTED]

[REDACTED] is a job aid used to execute the changing of passwords on [REDACTED] BES Cyber Assets in the [REDACTED]

Applicable Sections of the documented processes:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Detective Internal Controls involved? None

Preventative Internal Controls involved?

Preventative control- BES Cyber Assets are marked with a Pink Label stating NERC CIP as a compliance reminder.

PRIVILEGED AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Preventative Control - A Transient Cyber Asset was located in the [REDACTED] and marked with red labels identifying them as a device authorized for communications with CIP cyber devices.

Preventative Control - The personally assigned Corporate Laptops that were connected to the BES Cyber Asset were marked with yellow labels identifying them as not permitted for communications with CIP Cyber devices.

Preventative Control- [REDACTED] conducted visits to locations where [REDACTED] techs were performing work on 3/13/17. [REDACTED] conducted interviews of [REDACTED] techs to assess the employees training retention on proper use of TCAs.

#### Summary

While performing password changes at a medium impact BES site, two employees (authorized TCA users) connected their [REDACTED] corporate issued laptops to BES Cyber Assets. The employee's [REDACTED] issued laptops are not authorized as Transient Cyber Assets (TCAs) on [REDACTED] and do not have authorized users, locations, or uses identified. As a result, there is a possible violation of NERC CIP-010-2, R4 standard and requirement.

#### Timeline

On March 27 2017, training was provided covering NERC CIP-010-2, R4 standard/Requirement for NERC CIP Transient Cyber Assets (TCA) and Removable Media (RM).

On April 1 2017, NERC CIP-010-2, R4 standard/Requirement became enforceable that requires the use of authorized Transient Cyber Assets when connecting to BES Cyber Assets.

On July 26, 2017, at the [REDACTED] two [REDACTED] technicians (Tech 1 and Tech 2) decided to execute NERC CIP [REDACTED] password changes on the [REDACTED] at the site.

The technicians addressed that it was a NERC CIP site and completed a pre-job brief. Pre-job box for NERC CIP site is checked.

The technicians went to find the Job Plan [REDACTED] The technicians attempted to view the Job Plan in [REDACTED] but it was not attached to the work order;

A third technician was called to help locate the correct procedure. The procedure was found on the [REDACTED] site under [REDACTED]

Technician 1 casually reviewed the job plan to make sure it was the correct one for the planned work.

The technicians then began work at 1:40PM with their [REDACTED] issued laptops; not the dedicated CIP TCA laptop located at the site and mentioned in Step 1 of the Job Plan.

Part way through the task, at 3:00PM, Technician 1 moved to get a better position in front of another set of NERC CIP relays and noticed the CIP dedicated TCA laptop in the docking station located on the far end of the building from the entry door.

Realizing their mistake, both technicians stopped work immediately and notified their supervisor and waited for further instructions.

#### Causes of the violation

Apparent Cause #2 (AC2) -Human Errors or Inappropriate Actions/Inattention to Detail/Unawareness: Technicians overlooked the label on the corporate issued laptops stating "Not permitted for communication with CIP Cyber Devices" The Technicians overlooked step one of the job plan stating "Connect approved laptop to device. The laptop shall be on the approved Transient Cyber Asset inventory".

Contributing Cause #1 (CC1) -Human Errors or Inappropriate Actions/ Inattention to Detail/On the Job Distraction: Technicians had difficulty locating the password change [REDACTED] After searching in the [REDACTED] database they called another technician that was able to locate it.

Contributing Cause #2 (CC2) - Human Errors or Inappropriate Actions/Inadequate Mental State or Skills Too Complex/Lapse of Memory: Technicians failed to follow, NERC CIP Transient Cyber Assets (TCA) and Removable Media (RM) Information Session, training provided.

An Extent of Condition form was sent to all business areas [REDACTED] and responses are attached to the Discovery Tab of the [REDACTED] The [REDACTED] reviewed the EOC responses and details are below:

No other unauthorized devices were reported to have been connected to a NERC CIP device (BES Cyber Asset, BES Cyber Systems, PCAs)

The methodology used for the EOC was to look for preventative or detective controls being used the business area SME would assess the likely-hood of the control preventing an unauthorized TCA from being used.

The business areas listed in the [REDACTED] are representatives from [REDACTED]

[REDACTED] for this Self-Report  
[REDACTED] contains

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:

Part of requirement 4 of CIP-010 is to ensure appropriate authorization and use of specific Transient Cyber Assets (TCAs—laptops). The purpose of this requirement is to ensure appropriate security controls are applied to the devices, together with sufficient awareness and physical control of the devices are in place while connecting to BES Cyber Assets/Systems. The potential impact to the Bulk Electric System (BES) could be moderate if an adversary were successful in using an unauthorized transient device (laptop) to gain access to the devices (physical and/or electronic) because there is little if any way to know that appropriate security controls have been applied and are maintained on those devices.

Provide detailed description of Actual Risk to Bulk Power System:

While the devices that were connected to BES Cyber Assets/Systems were not authorized for use as CIP TCAs, they were authorized to perform work on the systems. As mitigating and compensating measures, [REDACTED] processes to ensure software, antivirus, and malware are updated were in place while the device were connected to the BCAs. Additionally, the corporate laptops that were connected to BCAs on 7/26/17 had antivirus updates [REDACTED] on 7/25/17 which would mitigate the introduction of malware to CIP BCAs. 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.

PRIVILEGED AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

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 43

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

43.a The Companies' Self-Report

43.b The Companies' Self-Report

43.c The Companies' Self-Report

43.d The Companies' Self-Report

43.e The Companies' Self-Report

43.f The Companies' Self-Report

This item was submitted by [REDACTED] on 6/23/2017

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

## FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

## REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-011-2

Applicable Requirement: [REDACTED]

R1.

Applicable Sub Requirement(s): [REDACTED]

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: 4/20/2017

Beginning Date of Possible Violation: 4/19/2017

End or Expected End Date of Possible Violation: 4/20/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-011-2, R1.2., the Responsible Entity shall establish procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.

Based on the NERC CIP Guidelines and Technical Basis, Requirement 1 states: "The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information."

On April 19, 2017 a [REDACTED] was working with the [REDACTED] on an issue related to the new rollout of [REDACTED] (the asset database used by [REDACTED] to manage BES cyber assets).

The vendor was not able to determine the cause of the error in a [REDACTED] session, so they requested a backup of the production [REDACTED] database being used and any .csv files the analyst was attempting to upload. The vendor wanted to recreate the environment to determine if they could reproduce the issue using the same data. The requested data was uploaded to the [REDACTED] via the [REDACTED] support website, using [REDACTED] for the file transfer.

On April 20, 2017 the [REDACTED] analyst remembered the data he sent to [REDACTED] was actually Production BES CSI Data. He immediately contacted [REDACTED] requesting that all [REDACTED] data uploaded to [REDACTED] the previous day be deleted.

That same day the vendor confirmed the data was deleted, had not been backed up, and was not viewed by anyone else at [REDACTED]

A Non-Disclosure Agreement (NDA) between [REDACTED] and [REDACTED] is in place which requires the vendor to treat all data with complete confidentiality and to properly destroy the data when troubleshooting efforts are completed.

The BES Cyber System and BES Cyber Assets associated with this potential violation is considered to be [REDACTED] because the BES CSI data sent to the vendor included production information for most, if not all, servers and datacenter appliances managed within the [REDACTED] database.

Steps implemented to resolve this potential violation were completed on 4/20/2017.

A cause analysis will be scheduled, along with creating a mitigation plan, to assist in preventing recurrence of this potential violation.



Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Severe

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 impact to the Bulk Electric System could potentially be severe should someone external to the company obtain this information and have access to the environment.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System because upon realizing the data sent to [REDACTED] was production BES CSI data, the [REDACTED] analyst contacted the [REDACTED] Senior Support Engineer requesting that all [REDACTED] data uploaded to [REDACTED] the previous day be deleted. That same day the vendor confirmed the data had been deleted, had not been backed up, and was not viewed by anyone else at [REDACTED]

Additional Comments:

Applies to: [REDACTED]

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 potential violation.

[REDACTED] management relevant to the situation actively participated and encouraged employees to provide complete information.

There have been no mis-operations, 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 6.4.)



This item was submitted by [REDACTED] on 8/3/2017

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:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

## REPORTING INFORMATION

Applicable Standard:

CIP-011-2

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.1.; 1.2.

Applicable Functions:

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:

6/23/2017

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: 6/30/2017

Beginning Date of Possible Violation: 6/30/2017

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

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per NERC CIP-011-2, Cyber Security – Information Protection:

R1.1, [REDACTED] is obligated to ensure information that meets the definition of Cyber System Information is clearly identified.

R1.2, [REDACTED] is obligated to ensure BES Cyber System Information is protected and securely handled when transmitting.

On Friday, June 30th, 2017, a [REDACTED] staff member (Project Manager) e-mailed information to a third party contractor that potentially included BES Cyber System Information (CSI) without labeling the information as such, or using a secure method to transmit the information.

The third party contractor requested the names of new [REDACTED] to complete a configuration step for which they were responsible. When the staff member responded to the third party contractor's request, a project document was attached that included the requested workstation names, but also several other pieces of BES cyber asset information.

During a follow up meeting with the third party contractor, approximately 2 hours after the information was delivered, it was realized that the document shared with them contained more than just the information requested. The [REDACTED] staff member failed to realize that the document attached contained the name of BES Cyber Assets [REDACTED], as well as, the location of future BES Cyber Assets [REDACTED]. Since the document contained BES CSI and was not labeled or communicated in a secure manner, the event was self-identified to have caused a possible violation.

The following mitigating activities have been completed:

1. A NERC CIP Stand Down call was conducted with all members of the [REDACTED] to convey the recently identified Possible Violation, as well as, the NERC CIP requirements to clearly identify BES Cyber System Information and use approved protection mechanisms when e-mailing BES Cyber System information outside [REDACTED]

- Completed 7/12/2017

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

2. [REDACTED] managers conducted follow-up staff meetings with their respective employees to discuss the key points of the NERC CIP Stand Down call. They reviewed a training package in the meetings that included the importance of clearly identifying BES Cyber System Information and the secure communication of this information. The training package included:

- a. Instructions on how to clearly label BES Cyber System Information per [REDACTED] requirements
- b. Instructions on how to [REDACTED] being sent outside of [REDACTED] that contains BES Cyber System Information
- c. Instructions on how to use [REDACTED]
- d. Instructions, via a process document, on how to [REDACTED] when secure FTP is not available

- Completed 7/12/2017

In order to prevent reoccurrence:

[REDACTED] T and Security managers will discuss and review with their staff the content of the training package that includes the importance of clearly identifying BES Cyber System Information and the secure communication of this information. This will be completed by 8/11/2017.

A cause analysis will be performed to identify additional actions required to prevent recurrence of this type of potential violation.



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 potential impact to the Bulk Power System is severe, due to the fact that identifying information, if obtained by someone with malicious intent, could have potentially been used to access systems that control the transmission grid in [REDACTED] resulting in the loss of utility.

Provide detailed description of Actual Risk to Bulk Power System:

There was no actual impact as a result of this possible violation. There were no misoperations, emergencies, or other adverse consequences to the Bulk Power System.

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 11/6/2017

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-004-6

Applicable Requirement:

R4.

Applicable Sub Requirement(s):

4.4.

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: 6/28/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 11/30/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per NERC CIP Standard CIP004-5: Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

Tracking of access to BES CSI repositories has recently (Q2 2017) been integrated into an automated platform within [REDACTED]. In June of 2017, a request was made to add an additional (new) repository and when determining access to that system, the requestor questioned what system administrator access would be captured within the system and whether there was a risk of a gap in the review process. During follow-up discussions with [REDACTED] on 6/28/2017, it was determined that administrator access was not being tracked within the system.

In order to evaluate the extent to which administrator access was captured for repositories, [REDACTED] conducted reviews of associated review procedures and previous completed access reviews, and conducted interviews with [REDACTED].

Examination of BES CSI Repository [REDACTED] reviews of [REDACTED] repositories across all business areas determined that the majority of [REDACTED] repositories [REDACTED] did not capture [REDACTED] administrator access. Further discussions with [REDACTED] personnel identified that system administrators such as [REDACTED] and database admins would be able to potentially access data on all systems administered. Across all [REDACTED] current BES Repositories the following groups with administrator access were identified:

During the Extent of Condition efforts, additional gaps in identifying BES CSI Repositories and the processes for authorizing and reviewing access to the Repositories were identified. The related Possible Violations are identified below and Cause Analysis efforts are currently underway for them in multiple Business Areas. Corrective Actions will be consolidated for these PV's into a single Mitigation Plan.

- Gap in tracking all Repository access within [REDACTED] system.
- Failure to identify all BES CSI Repositories.
- Training and PRA's Not Required for BES CSI Repository Access

In addition, non-production systems were determined to have production BES CSI data stored during phases of testing. Identification of these systems as repositories will be addressed with the corrective actions to identify all relevant BES CSI Repositories as documented within this analysis.

Overall, the Extent of Condition identified issues across the [REDACTED] with properly identifying BES CSI Repositories and fully identifying the access associated with them.



Interviews with [REDACTED] confirmed that there were instances of system level administrator access [REDACTED] that were not being captured as roles for BES CSI Repository access and subsequently not being reviewed by managers. The reviews confirmed that specific requests around capturing system administrator access were not made when submitting tickets to IT support for access lists. Reviews of [REDACTED] and business area procedures showed a lack of a clear process or guidelines on how to determine all access. [REDACTED] **Possible BES CSI Confidential Information HAS BEEN REDACTED FROM THIS PUBLIC VERSION** however, this is only applied to reviews of access [REDACTED]

to BES Cyber Assets and is not associated with BES CSI Repository reviews.

Based on reviews of the [REDACTED] platform and interviews with [REDACTED] the administrator access gap noted in the 2016 reviews was also not captured within [REDACTED]. The team relied on the previous manual review compilation of access lists and reviews with repository owners which were made up of business area representatives.

Based on the information gathered and reviewed, the causes identified for this issue were:

1. Direct Cause: Based on a Task Analysis, it was determined that there were no documented procedures or guidelines at the enterprise or business area level as to the requirements for capturing access including lack of defining that system administrator access should be captured by CIP Compliance groups to ensure system admin level access was documented.
2. Contributing Cause 1: Requests to IT for creating access reports did not always include specific instructions to include any access that might exist to the systems and associated BES CSI data and IT personnel were dependent upon CIP Compliance requests to define what access should be included per NERC CIP requirements. There was no engagement with IT groups administrating the systems to determine all access and any IT personnel fulfilling requests were reliant on what requirements were provided by Business Areas.
3. Contributing Cause 2: No central quality assurance review was performed to ensure correctness of access lists.
4. Contributing Cause 3: A time intensive manual effort with restricted resources and timeline led to incomplete data and lack of time to complete verification of data. [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:

From a potential harm standpoint, the repositories in question all contain sensitive information about BES Cyber Assets and could allow serious impact to the BES. With access, an individual with malicious intent would potentially be able to:

- Access sensitive information about BES Cyber Assets and their associated security configurations and controls and use it to compromise cyber asset security.

• [REDACTED]  
a [REDACTED]

In all of these cases, the individuals with access were [REDACTED] system administrators with a valid need to access the systems.

Provide detailed description of Actual Risk to Bulk Power System:

There was minimal likelihood that this event would adversely impact the Bulk Electric System for these reasons:

- All of these administrators do require access to the repositories based on their job functions; however, their access to the repositories was not reviewed and approved by their managers as required by [REDACTED] internal procedures. [REDACTED] of the [REDACTED] administrators identified have approved and current NERC CIP Personnel Risk Assessments (PRA's) which is above and beyond NERC CIP requirements for access to BES CSI Repositories. Although 5 of the domain administrators have not had PRA's completed, these approved administrative roles all have elevated rights to system platforms and therefore are trusted personnel expected to have access to sensitive information.

This gap could present a significant risk to the BES and result in operational impact. However, based on the reasons above, actual risk to the BES would be low due to this gap.

Additional Comments:

Although many of these personnel did have reviews completed for certain sites to which they had standard access, their administrator access for all repositories was not reviewed by managers. Based on reviews of the [REDACTED] platform and interviews with [REDACTED] the administrator access gap noted in the 2016 reviews was also not captured within [REDACTED] when repositories were integrated into the system.

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. A time intensive manual effort with restricted resources and timeline led to incomplete data and lack of time to complete verification of data. [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 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-011-2

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: [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: No

Date Possible Violation was discovered: 10/5/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 12/15/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED]. On October 5th 2017, [REDACTED] discovered that [REDACTED] was not considered in the initial identification of Bulk Electric System (BES) Cyber System Information (CSI) in Q4 of 2015 for CIP V5 implementation (effective date of July 1, 2016). Further evaluation of the information in [REDACTED] revealed that [REDACTED] containing BES CSI is stored in [REDACTED] and therefore, should have been identified as BES CSI during the initial identification. Although [REDACTED] are in place for [REDACTED] the failure to identify it as a BES CSI repository results in the inability to apply access authorization, provisioning and revocation controls and a possible violation of the above referenced standard and requirement.

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:

Identification and classification of BES CSI and BES CSI repositories is vital to ensure the appropriate security authorization, access and revocation controls are implemented to protect the information from compromise and subsequent misuse and potential degradation of BES Cyber Assets. As a result, the potential impact to the Bulk Electric System could be moderate if any such compromises took place because this repository contains BES Cyber Asset locations, IP Addresses and password information.

PRIVILEGED AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide detailed description of Actual Risk to Bulk Power System:

Although this repository was not previously identified and classified as BES CSI under the [REDACTED] CIP program, [REDACTED] Additionally, [REDACTED] has formally identified and classified this repository as BES CSI under our CIP program. These compensating controls provide mitigation to the potential impact and 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:

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]. In January 2017, [REDACTED] conducted a review of Electronic Access Control or Monitoring Systems (EACMS) used for authentication and/or authorization, where a "pool" of devices generally has equivalent ability to respond to authentication/authorization requests. This review was designed to ensure that, where [REDACTED] identifies an IT cyber asset as an EACMS, all of the equivalent devices are also correctly classified and protected.

This review identified that the [REDACTED] which can be used to log into devices that are in NERC CIP scope, had [REDACTED] servers that were not identified as EACMS. Based on the locations of these devices, they have performed EACMS functions for assets that are currently in NERC CIP scope and therefore should have been identified as EACMS. Device names are as follows:

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

The potential impact to the Bulk Power System was minimal. The devices reside physically within existing Physical Security Perimeters. User access to the is shared across all so existing access controls for users and administrators were enforced. User provisioning in the follows NERC CIP administration best practices, and the user population is limited to only personnel. Further, Finally, the Based on these security measures that were in place, 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.

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]

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] and [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:

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 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 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 [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.

POWERED 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 / documentation 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:

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



## Attachment 44

Record documents for the violation of CIP-011-2 R2

44.a Audit Summary

44.b The Companies' Self-Report

44.c The Companies' Self-Report



## 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]  
[REDACTED]

NERC Registry ID: [REDACTED]

Registered Entity Contact Information:

Name: [REDACTED]

Email: [REDACTED]

Standard: CIP-008-5

Requirement: R1

Sub Requirement(s):

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:

**Detailed explanation and cause of violation:** There is a single enterprise-wide high level Cyber Security Incident Response plan. This plan is a skeleton with no detail as to who is to do what task when and how. The Cyber Security Incident Response plan(s) is to be a detailed procedure people could follow to fully respond to Cyber Security Incidents and report them accurately to authorities.

**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 a cyber security incident occurs, personnel might not know what to do or who to contact to start an investigation or mitigation effort because the plan is too high level and overarching. Without detail the team must assemble, discuss the situation, and then have a leader start issuing orders to follow. Precious time will have elapsed before a proper response could be mounted.

**Detailed description of Actual Risk to Bulk Power System:** The personnel assigned to handle various tasks know their duties and would proceed to properly investigate, contain, and mitigate any incident.

**Additional Comments:** Since this is the enterprise-wide [REDACTED] plan then it spreads across all registered entities for CIP since this is the plan they would use in the event of a cyber security incident.

[REDACTED]  
[REDACTED]  
[REDACTED].

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

---

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

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:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

## REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.1.

Applicable Functions:

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]. In January 2017, [REDACTED] conducted a review of Electronic Access Control or Monitoring Systems (EACMS) used for authentication and/or authorization, where a "pool" of devices generally has equivalent ability to respond to authentication/authorization requests. This review was designed to ensure that, where [REDACTED] identifies an IT cyber asset as an EACMS, all of the equivalent devices are also correctly classified and protected.

This review identified that the [REDACTED] which can be used to log into devices that are in NERC CIP scope, had three [REDACTED] servers that were not identified as EACMS. Based on the locations of these devices, they have performed EACMS functions for assets that are currently in NERC CIP scope and therefore should have been identified as EACMS. Device names are as follows:

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

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

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. The three devices reside physically within existing Physical Security Perimeters. User access to the [REDACTED] is shared across [REDACTED] so existing access controls for [REDACTED] users and administrators were enforced. User provisioning in the [REDACTED] follows NERC CIP administration best practices, and the user population is limited to only [REDACTED] personnel. Further, the [REDACTED] reside behind Firewalls in [REDACTED] networks. Finally, the [REDACTED] suite of tools and best practices were used when the systems were commissioned, [REDACTED]. Based on these security measures that were in place, 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:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

## REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1a

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.1.

Applicable Functions:

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:

4/7/2017

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:

If yes, indicate which Region(s):

Date Reported to Region(s):

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

Seven [REDACTED] and two [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:

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 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.

[REDACTED] firewall rules, focused on systems designed to facilitate IRA and were incorrectly implemented due to the lack of clarity

A

d? 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] 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 and non-CONFIDENTIAL

HAS BEEN REDACTED FROM THIS PUBLIC VERSION

See section ██████████ Recommended by ██████████ 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 ██████████ business procedures and the updated ██████████ documentation
- With oversight from ██████████ all ██████████ to provide a draft of ██████████ 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 ██████████ business level procedures
- With oversight from ██████████ all ██████████ to communicate and provide training on updated ██████████ 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.

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





## Attachment 45

Record documents for the violation of CIP-014-2 R1

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

45.b The Companies' Certification of Mitigation Plan Completion.

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-014-2

Applicable Requirement: R2.

Applicable Sub Requirement(s): [REDACTED]

Applicable Functions: [REDACTED]

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

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

Date Possible Violation was discovered: 4/25/2016

Beginning Date of Possible Violation: 10/2/2015

End or Expected End Date of Possible Violation: 9/30/2016

Is the violation still occurring? No

## Provide detailed description and cause of Possible Violation:

During the fall 2015 CIP-014-2 R1 assessment, [REDACTED] ran physical security analysis for [REDACTED] stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1.

Upon further scrutiny during the week of April 25, 2016, however, it was determined that [REDACTED] had not been run in the final analysis that was shared with the unaffiliated third party verifier for R2. [REDACTED]

[REDACTED] was run in preliminary analysis by [REDACTED] and was not found to have adverse results requiring inclusion on the physical security protection list for the purpose of CIP-014-2. Failure to include [REDACTED] in the final analysis shared with the unaffiliated third party verifier, however, may possibly constitute a violation of R2.

Are Mitigating Activities in progress or completed? Yes

## If Yes, Provide description of Mitigating Activities:

- 1) Run [REDACTED] in a special assessment ASAP, and share with the unaffiliated third party verifier. Completed on 6/17/2016
- 2) Revisit CIP-014-2 best practices with other [REDACTED] peers. To be completed 8/29/2016.
- 3) Modify and republish [REDACTED] to incorporate the proposed approach in (1) above (refer to (1) in details to prevent recurrence). To be completed by 9/30/2016.

## Provide details to prevent recurrence:

- 1) In future assessments, run all [REDACTED] stations and substations to be shared with the unaffiliated third party verifier, making no exclusions for Applicability Section 4.1.1. Have the unaffiliated third party verifier a) review all analysis results and b) verify accuracy of [REDACTED] application of Applicability Section 4.1.1 via a [REDACTED] program contingency report using the present-day and 24-months-out base cases as well as the system one-line diagrams.
- 2) Modify and republish [REDACTED] CIP-014-2 Methodology to incorporate the proposed approach in (1) above (refer to (1) in details to prevent recurrence). To be completed by 9/30/2016.

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

9/30/2016

**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:

[REDACTED] was run in preliminary analysis by [REDACTED] and was not found to have adverse results requiring inclusion on the physical security protection list for the purpose of CIP-014-2. Following the discovery of this PV, the analysis was re-run and shared with the unaffiliated third party verifier, and was again not found to have adverse results requiring inclusion on the physical security protection list for the purpose of CIP-014-2. Given these two facts, there is no Potential Impact to the Bulk Power System.

Provide detailed description of Actual Risk to Bulk Power System:

The actual impact to the Bulk Power System (BPS) was minimal. During the duration of non-compliance there were no instances where [REDACTED] Facilities that were rendered inoperable or damaged as a result of a physical attack.

Additional Comments:

THIS PV is being submitted for [REDACTED] via [REDACTED] portal.

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 signed by [REDACTED] on 8/25/2017

This item was marked ready for signature by [REDACTED] on 8/25/2017

## MEMBER MITIGATION PLAN CLOSURE

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

Name of Registered Entity submitting certification:

Name of Standard of mitigation violation(s):

CIP-014-2

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

Date of completion of the Mitigation Plan:

9/30/2016

1. Run Special Assessment

Milestone Completed (Due: 7/31/2016 and Completed 6/17/2016)

[Attachments \(0\)](#)

Run [REDACTED] substation in a special assessment and share with the unaffiliated third party verifier.

2. Revisit best practices

Milestone Completed (Due: 9/1/2016 and Completed 8/29/2016)

[Attachments \(0\)](#)

Revisit CIP 014 2 best practices with other [REDACTED]

3. Modify and republish Methodology

Milestone Completed (Due: 9/30/2016 and Completed 9/30/2016)

[Attachments \(0\)](#)

Modify and republish [REDACTED] CIP 014 2 Methodology to incorporate the proposed approach stated in Section D 1 of the Mitigation Plan.

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

[REDACTED] ran a special assessment and shared it with the unaffiliated third party, revisited Best Practices and modified and republished its Methodology.

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

Evidence will be provided on site if [REDACTED] wishes to review such.

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