Attachment 13

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

13.a The Entity's Self-Report (RFC2017017546);
13.b The Entity's Mitigation Plan designated as RFCMIT012908 submitted [redacted];
13.c The Entity's Certification of Mitigation Plan Completion dated [redacted];
13.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted];
13.e The Entity's Self-Report (RFC2017017765);
13.f The Entity's Mitigation Plan designated as RFCMIT013013 submitted [redacted];
13.g The Entity's Certification of Mitigation Plan Completion dated [redacted];
13.h ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted];
13.i The Entity's Self-Report (RFC2017017840);
13.j The Entity's Mitigation Plan designated as RFCMIT013022-1 submitted [redacted];
13.k The Entity's Certification of Mitigation Plan Completion dated [redacted];
13.l ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted];
13.m The Entity's Self-Report (RFC2017018307);
13.n The Entity's Mitigation Plan designated as RFCMIT013267 submitted [redacted];
13.o The Entity's Certification of Mitigation Plan Completion dated [redacted];
13.p ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted];
13.q The Entity's Self-Report (RFC2018019647);
13.r The Entity's Mitigation Plan designated as RFCMIT013784-1 submitted [redacted];
13.s The Entity's Certification of Mitigation Plan Completion dated [redacted];
13.t ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted]

Self Report

Entity Name:
NERC ID:
Standard: CIP-002-5.1
Requirement: CIP-002-5.1 R1.
Changed to CIP-010-2 R1
Date Submitted:
Has this violation previously been reported or discovered?: No

Entity Information:

Joint Registration Organization (JRO) ID:
Coordinated Functional Registration (CFR) ID:
Contact Name:
Contact Phone:
Contact Email:

Violation:

Violation Start Date: September 29, 2016
End/Expected End Date:
Reliability Functions:
Is Possible Violation still occurring?: No
Number of Instances: 1
Has this Possible Violation been reported to other Regions?: No
Which Regions:
Date Reported to Regions:

Detailed Description and Cause of Possible Violation: Incident 1
As of July 1, 2016, came into scope as asset. New assets were not added to the ESP (Electronic Security Perimeter) until May 2016 when a change order was opened and approved to add PCA assets. These are management consoles for managing all NERC CIP assets at the Required approvals on the change order were completed by 5/17/16. Network operations configured an access point VLAN on a switch on 9/29/16. The workstations were connected to the network on 9/29/16 after the VLAN was created. Existing firewall rules as of 9/29/16 would have permitted remote access to the workstations via the jump server after they were connected. The PCA assets were later discovered to have been installed using basic operating systems image without any hardening.
The workstations were granted access through the firewall to the and networks on 10/14/16. The workstations were granted access through the firewall to the network on 11/7/16.
Possible non-compliance:
CIP-007 R1.1: Prior to placing these assets in production, the firewalls were not enabled violating CIP 007 R1.1.
CIP-007 R2.1, 2.2, 2.3: The patch sources of these assets were neither identified nor evaluated after being placed into production violating CIP 007 R2.1 and R2.2. PCA assets were not patched between September 2016 and February 2017, violating CIP-007 R2.3.

CIP-007 R5.3: Shared accounts were not inventoried and individuals who have access to these assets were not identified which was a violation of CIP-007 R5.3.
CIP-010 R1.1: A notification to create a baseline was not done and therefore no baseline existed for these [redacted] assets violating CIP 010 requirement 1.
CIP-010 R3: A vulnerability assessment was not completed prior to implementation into production which was violation of CIP 010 requirement 3.
In conclusion, these [redacted] PCA assets were not added to the BES cyber system list in a timely manner. One control to detect such events is the semi-annual walk down process. The procedure requires comparison of physical assets to the asset list. However, the BES Cyber walk down for the [redacted] was held in early September before the assets were added. The next walk down was held on March 21, 2017, during which this issue was found and reported.
During [redacted] ([redacted] and Root Cause Analysis (RCA), we learned that [redacted] group is a technology group that is responsible for installing hardware in the network and corporate IT is responsible for installing network equipment. There is no documented process describing the responsibilities of the two groups. It was also noted that change control process uses ServiceDesk, which assigns change order tasks to each responsible SME. The tasks assigned in this case were assigned to [redacted] technicians who were not set up to receive an email when task is assigned to them. As a result, they were not aware and could not carry out the assigned task in a timely manner.
To prevent the reoccurrence of this issue, it was decided that the [redacted] group needed to undergo a refresher training on the change control policies for NERC devices and how to carry out changes to NERC assets in a compliant manner.
Two individuals who installed the workstations were identified and were coached by their supervisor immediately.

Incident 2
On 10/17/2016, a [redacted] BCA asset the [redacted] in [redacted] room failed. This failed server required immediate replacement because of possible impact to BES Cyber System functionality. Therefore, an urgent change order [redacted] was opened to replace the failed server. The change control procedure allows urgent changes to be carried out without prior approval. However, the approval must be obtained the next day. The work order was not approved in the [redacted] the following day as required due to lack of a designated manager. As a result, the following verification controls in the [redacted] ([redacted] were not completed: 1) recording configuration baselines, 2) vulnerability assessment prior to the equipment being installed, 3) updating the metadata in the BES asset list, 4) generating the baseline for the new asset, 5) validating that the new asset configuration matches the failed asset and 6) current patches were not applied or mitigated. It was also further noted that an exceptional circumstance could have been executed by the SMEs on site in order to replace the failed server that required immediate replacement. The BCA server was later noted to have been installed using basic operating systems image without any hardening.
Possible non-compliance:
CIP-007 R2.1, 2.2, 2.3: The patch sources for these assets were not identified nor were patches evaluated before being placed into production. This violates CIP-007 R2.1 and R2.2. By not patching between September 2016 and February 2017 it violates CIP-007 R2.3.
CIP-007 R5.3: Shared accounts were not inventoried and individuals who have access to these assets were not identified which was a violation of CIP-007 R5.3.
CIP-010 R1.1: A notification to create a baseline was not done and therefore no baseline existed for this asset violating CIP 010 requirement 1.
CIP-010 R3: A vulnerability assessment was not completed prior to implementation into production which is a violation of CIP 010 requirement 3.
After the discovery of this issue, the business unit obtained formal approval from [redacted] on 3/15/2017. And the asset was added to the BES Cyber Systems list on 3/16/2017.
An [redacted] conducted on 3/13/2017 determined the lack of a timely

[redacted] approval to be a reportable possible violation of CIP-010 R1. A follow up task designated someone to approve such change orders for the [redacted]
After the [redacted] approval was obtained, the business unit conducted an exercise on 3/24/2017 to verify that all required tasks related to the change, as listed above, were completed in a compliant manner. Following the verification exercise, the [redacted] Change Control Board concluded the change order as completed. The change order was closed on 4/3/2017.

Root Cause of Possible Violation:
Workflow failures - The root cause of this violation in both noted incidents is the ineffective use of the change control system for the added assets. The change system was not set up with an approval manager for [redacted]
Furthermore, there was no escalation to get the CO approved. Also, SMEs needed to complete cybersecurity tasks were not set up with email addresses to receive assignments.
Human Performance failure - In addition, SMEs of [redacted] group at [redacted] have completed training but failed to follow the change procedures because asset additions are infrequent.
Process Control missing - [redacted] process lacked a control to look for old and non-approved change orders with completion issues.
The recovery plan for the BCA asset was not used in replacing the faulty server in case of instance 2.

How was the violation discovered?
First violation was discovered when [redacted] performed a new control to review all open change orders older than 30 days. In the course of the review, an open change order was found to still be open since May, 2016. Upon investigating why the change order remained open, it was discovered that in the process of adding the PCA assets, the change control process was not followed leading to critical change control steps and documentation not being performed.
Second violation was discovered during an [redacted] routine QA review of asset destruction process. An asset was found in the destruction bin located within the [redacted] PSP. The asset destruction logs showed the asset was appropriately logged for destruction, but the related work order did not have a completion date and the required approval recorded.

Timeline:
Incident 1
May 3, 2016 Change Order (CO) was opened/ approved to add PCA networking assets.
July 1, 2016 [redacted] became NERC CIP [redacted] asset.
September 13, & September 14, 2016 BES Cyber walk-down for [redacted]
September 9, 2016 Task for IT to enable necessary network ports, to connect to ESP was opened
September 29, 2016 [redacted] workstations were added (connected to the network) to [redacted] ESP
October 14, 2016 Workstations were granted access through the firewall to the [redacted] and [redacted] networks
November 7, 2016 Workstations were granted access through the firewall to the [redacted] network
February 2, 2017 Tasks related to the [redacted] Firewall was completed and closed upon verification by [redacted]
February 28, 2017 [redacted] receives notification about the violation.
March 3, 2017 [redacted] closed and approved based on evidence for February 2, 2017
March 8, 2017 Change Order was deemed as successfully completed therefore closed.

Incident 2
10/17/2016 Critical [redacted] server failed and an urgent change request was created to replace.
10/17/2016 Business Unit IT manager approved Change Order request

10/18/2017 Initial [redacted] Approval request was denied because appropriate secondary approval was not obtained
February 2017 [redacted] performed QA review of Asset Destruction Process which yielded this possible violation.
3/15/2017 [redacted] approval was obtained
3/16/2017 BES Cyber System list was updated with change performed
3/24/2017 Business unit verified change evidence against required change control process to ensure all required steps were completed in accordance with the IT Change Control Process.
4/3/2017 [redacted] Change Control Board approvers conclude change successfully completed and the change order [redacted] was formally closed.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Mitigating Activities:
Incident 1
- Coached [redacted] employees on the use of change control for adding, modifying, or removing a NERC asset
- A refresher training on the change control process was given to the employees who added the assets.
- Worked with the change process leader to set up service desk for sending emails to [redacted] SMEs when a new task is assigned or created so that they know what, when, and how to complete the task created/assigned.

Incident 2
The business unit obtained all required approvals and they performed the required change control measures listed in the description section above. The change order was appropriately closed after being deemed as successfully completed by the [redacted]

Preventive Measures:
Incident 1 Document the process and responsibilities of [redacted] ([redacted] and/or IT work on installing new assets
Incident 2
To prevent the recurrence of this violation, the business unit designated a secondary manager to approve future urgent change requests in a timely manner.
A weekly change review at the business unit level has been initiated to review all active change orders to ensure they are either progressing according to plan or closed. This review will also serve as a forum to ensure all critical change control measures and documentation are completed as required.
Additionally, the [redacted] process has been updated to ensure change orders are either approved or denied within 30 days.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: The potential impact of these non-compliant changes around PCA and BCA assets is deemed as moderate because, while the assets were installed from a less secured image without any hardening applied to them upon installation, up to date patches were not applied before implemented into production and the assets were also not included in the asset lists; all these conditions creates vulnerabilities that makes it easier for even an unsophisticated attacker to compromise any of the assets. The business unit is overall classified as a moderate risk facility to the organization.
The actual impact of this violation to the BES is deemed to be lower VSL because compensating controls in place such as robust access and identity management, effective monitoring of added assets every 30 days, review of

configuration baselines every 35 days and regular QA of these controls to ensure they are operating effectively would make the task of an attacker difficult; hence, the BES was not recorded to have suffered any damage as a result of the violations.

Risk Assessment of Impact to BPS: The impact of this risk to the BES is assessed to be low because of the operating effectiveness of the aforementioned compensating controls and the fact that the BES did not suffer any recorded disruption or security breach as a result of the changes made.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017017546	CIP-002-5.1 R1.	**Changed to CIP-010-2 R1**

Mitigation Plan Submitted On [redacted]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: June 20, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

(1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
(2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
(3) The cause of the Alleged or Confirmed Violation(s).
(4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
(5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
(6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
(7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
(8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
(9) Any other information deemed necessary or appropriate.
(10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
(11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

• The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.

• This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.

• If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.

• Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.

• Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.

• The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [redacted]

NERC Compliance Registry ID: [redacted]

Address: [redacted]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017017546	09/29/2016	CIP-002-5.1 R1.
Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:[See Standard for sub-req's]		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

Brief Description: (What happened?)
Incident 1:
As of July 1, 2016, [redacted] came into scope as [redacted] asset. New assets were not added to the [redacted] ESP (Electronic Security Perimeter) until May 2016 when a change order was opened and approved to add [redacted] PCA assets. These are management consoles for managing all NERC CIP assets at the [redacted] Required approvals on the change order [redacted] were completed by 5/17/16. Network operations configured an access point [redacted] on a switch on 9/29/16. The workstations were connected to the network on 9/29/16 after the VLAN was created. Existing firewall rules as of 9/29/16 would have permitted remote access to the workstations via the [redacted] after they were connected. The PCA assets were later discovered to have been installed using basic operating systems image without any hardening. The workstations were granted access through the firewall to the [redacted] and [redacted] networks on 10/14/16. The workstations were granted access through the
firewall to the [redacted] network on 11/7/16.

Possible non-compliance:
CIP-007 R1.1: Prior to placing these assets in production, the firewalls were not enabled violating CIP 007 R1.1.
CIP-007 R2.1, 2.2, 2.3: The patch sources of these assets were neither identified nor evaluated after being placed into production violating CIP 007
R2.1 and R2.2. PCA assets were not patched between September 2016 and February 2017, violating CIP-007 R2.3.
CIP-007 R5.3: Shared accounts were not inventoried and individuals who have access to these assets were not identified which was a violation of CIP-007
R5.3.
CIP-010 R1.1: A notification to create a baseline was not done and therefore no baseline existed for these two assets violating CIP 010 requirement 1.
CIP-010 R3: A vulnerability assessment was not completed prior to implementation into production which was violation of CIP 010 requirement 3.

In conclusion, these two PCA assets were not added to the BES cyber system list in a timely manner. One control to detect such events is the semi-annual walk down process. The procedure requires comparison of physical assets to the asset list. However, the BES Cyber walk down for the [redacted] was held in early September before the assets were added. The next walk down was held on March 21, 2017, during which this issue was found and reported.

Incident 2:
On 10/17/2016, a [redacted] BCA asset the [redacted] in [redacted] room failed. This failed server required immediate replacement because of possible impact to BES Cyber System functionality. Therefore, an urgent change order [redacted] was opened to replace the failed server. The change control procedure allows urgent changes to be carried out without prior approval. However, the approval must be obtained the next day. The work order was not approved in the [redacted] ([redacted] the following day as required due to lack of a designated manager. As a result, the following
verification controls in the [redacted] ([redacted] were not completed: 1) recording configuration baselines, 2) vulnerability assessment prior to the equipment being installed, 3) updating the metadata in the BES asset list, 4) generating the baseline for the new asset, 5) validating that the new asset configuration matches the failed asset and 6) current patches were not applied or

mitigated. It was also further noted that an exceptional circumstance could have been executed by the SMEs on site in order to replace the failed server that required immediate replacement. The BCA server was later noted to have been installed using basic operating systems image without any hardening.

Possible non-compliance:
CIP-007 R2.1, 2.2, 2.3: The patch sources for these assets were not identified nor were patches evaluated before being placed into production. This violates CIP-007 R2.1 and R2.2. By not patching between September 2016 and February 2017 it violates CIP-007 R2.3.
CIP-007 R5.3: Shared accounts were not inventoried and individuals who have access to these assets were not identified which was a violation of CIP-007 R5.3.
CIP-010 R1.1: A notification to create a baseline was not done and therefore no baseline existed for this asset violating CIP 010 requirement 1.
CIP-010 R3: A vulnerability assessment was not completed prior to implementation into production which is a violation of CIP 010 requirement 3.
After the discovery of this issue, the business unit obtained formal approval from [redacted] on 3/15/2017. And the asset was added to the BES Cyber Systems list on 3/16/2017.

Cause: (what caused the violation?)

Incident 1: During [redacted] ([redacted] and [redacted] ([redacted] we learned that [redacted] ([redacted] group is a technology group that is responsible for installing hardware in the network and corporate IT is responsible for installing network equipment. There is no documented process describing the responsibilities of the two groups. It was also noted that change control process uses Service Desk, which assigns change order tasks to each responsible SME. The tasks assigned in this case were assigned to [redacted] technicians who were not set up to receive an email when task is assigned to them. As a result, they were not aware and could not carry out the assigned task in a timely manner. To prevent the reoccurrence of this issue, it was decided that the [redacted] group needed to undergo a refresher training on the change control policies for NERC devices and how to carry out changes to NERC assets in a compliant manner.

Incident 2: An [redacted] conducted on 3/13/2017 determined the lack of a timely [redacted] approval to be a reportable possible violation of CIP-010 R1. A follow up task designated someone to approve such change orders for the [redacted]

The root cause for these two incidents are listed below:

Workflow failures - The root cause of this violation in both noted incidents is the ineffective use of the change control system for the added assets. No [redacted] personnel were given manager level approval in service desk to approve the change orders. Furthermore, there was no escalation to get the CO approved. Also, SMEs needed to complete cybersecurity tasks were not set up with email addresses to receive assignments.
Human Performance failure - In addition, SMEs of [redacted] group at [redacted] have completed training but failed to follow the change procedures because asset additions are infrequent.
Process Control missing - [redacted] process lacked a control to look for old and non-approved change orders with completion issues.

Timeline:
Incident 1
May 3, 2016 Change Order (CO) was opened/ approved to add PCA networking assets.
July 1, 2016 [redacted] became NERC CIP [redacted] asset.
September 13, & September 14, 2016 BES Cyber walk-down for [redacted]
September 9, 2016 Task for IT to enable necessary network ports, to connect to ESP was opened
September 29, 2016 [redacted] workstations were added (connected to the network) to [redacted] ESP
October 14, 2016 Workstations were granted access through the firewall to the [redacted] and [redacted] networks
November 7, 2016 Workstations were granted access through the firewall to the [redacted] network
February 2, 2017 Tasks related to the [redacted] Firewall was completed and closed upon verification by [redacted]
February 28, 2017 [redacted] receives notification about the violation.
March 3, 2017 [redacted] closed and approved based on evidence for February 2, 2017
March 8, 2017 Change Order was deemed as successfully completed therefore closed.

Incident 2
10/17/2016 Critical [redacted] server failed and an urgent change request was created to replace.
10/17/2016 [redacted] approved Change Order request
10/18/2017 Initial [redacted] Approval request was denied because appropriate secondary approval was not obtained
February 2017 [redacted] performed QA review of [redacted] which yielded this possible violation.
3/15/2017 [redacted] approval was obtained
3/16/2017 BES Cyber System list was updated with change performed
3/24/2017 Business unit verified change evidence against required change control process to ensure all required steps were completed in accordance with the IT [redacted].
4/3/2017 [redacted] approvers conclude change successfully completed and the change order CO25659 was formally closed.

Relevant information regarding the identification of the violation(s):

How was the violation discovered?

Incident 1:
First violation was discovered when [redacted] performed a new control to review all open change orders older than 30 days. In the course of the review, an open change order was found to still be open since May, 2016. Upon investigating on why the change order remained open, it was discovered that in the process of adding the PCA assets, the change control process was not followed leading to critical change control steps and documentation not being performed.

Incident 2:
Second violation was discovered during an [redacted] routine QA review of asset destruction process. An asset was found in the destruction bin located within the [redacted] PSP. The asset destruction logs showed the asset was appropriately logged for destruction, but the related work order did not have a completion date and the required approval recorded.

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

Milestone 1- [redacted] configured service desk to send out emails to the Subject Matter Experts (SME's) and managers. The purpose of this milestone is so that all the managers and SMEs get a notification and they will know when a task is assigned to them. The outcome will be to receive notifications which will lead to completing the tasks faster and reducing potential non-compliance.

Milestone 2 - [redacted] conducted a deep dive process review of the change control process and procedures with all the [redacted] SMEs. The purpose of this milestone is to have a better understanding of the process to resolve the lack of knowledge of the process, and reduce the potential non-compliance issue of this standard or similar standards.

Milestone 3 - [redacted] is working towards bringing assets identified in this self report in compliance with all the applicable standards. The purpose of this milestone is to identify and obtain all the approvals and to complete and close all the change orders appropriately. This will ensure completion with proper procedure followed, and will reduce potential non-compliance for the standards.

Milestone 4- [redacted] also updated [redacted] process to include review of change orders open for more than 30 days. The purpose of this milestone is to ensure that there are no change orders avoided and are taken care of accordingly on time. This will reduce potential non-compliance by reviewing these tasks every week to see if they need escalation.

Milestone 5 - [redacted] will be adding a proper documentation for [redacted] and IT when adding new assets. The purpose of this milestone is to ensure that the [redacted] and IT group know what their responsibilities are when adding new assets to the system. This will prevent future potential noncompliance issues as it is a documented process which will eventually eliminate the lack of knowledge on how to add the assets.

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: June 20, 2017

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Configure [redacted] to send emails to [redacted] SMEs	Configure [redacted] to include [redacted] SME's and Managers so that they can receive emails when a work item is assigned.	04/20/2017	04/20/2017		No
Deep Dive of the change control application used in	Deep dive process review to understand the change control	05/17/2017	05/17/2017		No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
[redacted]	process. This will be performed by using application.				
Assets in compliance to all applicable requirements.	Business unit obtained all required approvals and they performed the required change control measures listed. The change order was appropriately closed after being deemed as successfully completed by the [redacted]	05/24/2017			No
Process Documentation	Document the process and responsibilities of [redacted] and or IT work on installing new assets	05/30/2017			No
[redacted] update	[redacted] process to be updated to include review of open Change Orders (CO's) older than 30 days	06/15/2017			No

Additional Relevant Information

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

[redacted] has delivered a verbal communication to follow the change control process which was later followed up by the deep dive on 3/16/2017.

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

The successful completion of the Mitigation Plan will minimize the probability of further violation of same or similar standards by completing a thorough review of the process to ensure proper understanding of the change control process, configuring emails to send out when a work is assigned, ensuring all the assets are in compliance with the standards, implementing a process for [redacted] to review open change orders older than 30 days, and also documenting a clear process to explain the responsibilities of [redacted] and IT in adding new assets. These mitigating activities, once completed, shall minimize or even prevent future violations of same or similar standards.

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.

2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.

3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

[redacted] Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: [redacted]

Title: [redacted]

Authorized On: [redacted]

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request 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)

Registered Entity Name: [redacted]
NERC Registry ID: [redacted]
NERC Violation ID(s): RFC2017017546
Mitigated Standard Requirement(s): CIP-002-5.1 R1. **Changed to CIP-010-2 R1**
Scheduled Completion as per Accepted Mitigation Plan: June 20, 2017
Date Mitigation Plan completed: July 17, 2017
RF Notified of Completion on Date: [redacted]
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017546 Certification Package.zip	File "RFC2017017546 Certification Package.zip" contains cover page for the package and also supporting evidence for each milestone.	14,534,821
Entity	File 2 Milestone 3.pdf		13,412,338
Entity	File 3 Milestone 4.pdf		3,527,825
Entity	File 4 Milestone 5.pdf		2,265,844

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Mitigation Plan Verification for RFC2017017546

[redacted] ([redacted])

Standard/Requirement: CIP-002-5.1 R1 **Changed to CIP-010-2 R1**

NERC Mitigation Plan ID: RFCMIT012908

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	07/17/17

Description of Issue

Incident 1:

As of July 1, 2016, [redacted] came into scope as [redacted] asset. New assets were not added to the [redacted] ESP (Electronic Security Perimeter) until May 2016 when a change order was opened and approved to add [redacted] PCA assets. These are management consoles for managing all NERC CIP assets at the [redacted] Required approvals on the change order [redacted] were completed by 5/17/16. Network operations configured an access point VLAN on a switch on 9/29/16. The workstations were connected to the network on 9/29/16 after the VLAN was created. Existing firewall rules as of 9/29/16 would have permitted remote access to the workstations via the [redacted] after they were connected. The PCA assets were later discovered to have been installed using basic operating systems image without any hardening. The workstations were granted access through the firewall to the [redacted] and [redacted] networks on 10/14/16. The workstations were granted access through the firewall to the [redacted] network on 11/7/16.

Possible non-compliance:

CIP-007 R1.1: Prior to placing these assets in production, the firewalls were not enabled violating CIP 007 R1.1. CIP-007 R2.1, 2.2, 2.3: The patch sources of these assets were neither identified nor evaluated after being placed into production violating CIP 007

R2.1 and R2.2. PCA assets were not patched between September 2016 and February 2017, violating CIP-007 R2.3.

CIP-007 R5.3: Shared accounts were not inventoried and individuals who have access to these assets were not identified which was a violation of CIP-007

R5.3.

CIP-010 R1.1: A notification to create a baseline was not done and therefore no baseline existed for these two assets violating CIP 010 requirement 1.

CIP-010 R3: A vulnerability assessment was not completed prior to implementation into production which was violation of CIP 010 requirement 3.

In conclusion, these [redacted] PCA assets were not added to the BES cyber system list in a timely manner. One control to detect such events is the semi-annual walk down process. The procedure requires comparison of physical assets to the asset list. However, the BES Cyber walk down for the [redacted] was held in early September before the assets were added. The next walk down was held on March 21, 2017, during which this issue was found and reported.

Incident 2:

On 10/17/2016, a [redacted] BCA asset the [redacted] in [redacted] room failed. This failed server required immediate replacement because of possible impact to BES Cyber System functionality. Therefore, an urgent change order [redacted] was opened to replace the failed server. The change control procedure allows urgent changes to be carried out without prior approval. However, the approval must be obtained the next day.

The work order was not approved in the [redacted] ([redacted] the following day as required due to lack of a designated manager. As a result, the following

verification controls in the [redacted] ([redacted] were not completed: 1) recording configuration baselines, 2) [redacted] prior to the equipment being installed, 3) updating the metadata in the BES asset list, 4) generating the baseline for the new asset, 5) validating that the new asset configuration matches the failed asset and 6) current patches were not applied or mitigated. It was also further noted that an exceptional circumstance could have been executed by the SMEs on site in order to replace the failed server that required immediate replacement. The BCA server was later noted to have been installed using basic operating systems image without any hardening.

Possible non-compliance:

CIP-007 R2.1, 2.2, 2.3: The patch sources for these assets were not identified nor were patches evaluated before being placed into production. This violates CIP-007 R2.1 and R2.2. By not patching between September 2016 and February 2017 it violates CIP-007 R2.3.

CIP-007 R5.3: Shared accounts were not inventoried and individuals who have access to these assets were not identified which was a violation of CIP-007 R5.3.

CIP-010 R1.1: A notification to create a baseline was not done and therefore no baseline existed for this asset violating CIP 010 requirement 1.

CIP-010 R3: A vulnerability assessment was not completed prior to implementation into production which is a violation of CIP 010 requirement 3.

After the discovery of this issue, the business unit obtained formal approval from [redacted] on 3/15/2017. And the asset was added to the BES Cyber Systems list on 3/16/2017.

Cause: (what caused the violation?)

Incident 1: During [redacted] ([redacted] and [redacted], we learned that [redacted] ([redacted] group is a technology group that is responsible for installing hardware in the network and corporate IT is responsible for installing network equipment. There is no documented process describing the responsibilities of the two groups. It was also noted that change control process uses Service Desk, which assigns change order tasks to each responsible SME. The tasks assigned in this case were assigned to [redacted] technicians who were not set up to receive an email when task is assigned to them. As a result, they were not aware and could not carry out the assigned task in a timely manner. To prevent the reoccurrence of this issue, it was decided that the [redacted] group needed to undergo a refresher training on the change control policies for NERC devices and how to carry out changes to NERC assets in a compliant manner.

Incident 2: An [redacted] conducted on 3/13/2017 determined the lack of a timely [redacted] approval to be a reportable possible violation of CIP-010 R1. A follow up task designated someone to approve such change orders for the [redacted]

The root cause for these two incidents are listed below:

Workflow failures - The root cause of this violation in both noted incidents is the ineffective use of the change control system for the added assets. No [redacted] personnel were given manager level approval in service desk to approve the change orders. Furthermore, there was no escalation to get the CO approved. Also, SMEs needed to complete cybersecurity tasks were not set up with email addresses to receive assignments.

Human Performance failure - In addition, SMEs of [redacted] group at [redacted] have completed training but failed to follow the change procedures because asset additions are infrequent.

Process Control missing - [redacted] process lacked a control to look for old and non-approved change orders with completion issues.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017017546 Certification Package	CIP-002-5.1 R1
File 2	Milestone 3	CIP-002-5.1 R1
File 3	Milestone 4	CIP-002-5.1 R1
File 4	Milestone 5	CIP-002-5.1 R1

Verification of Mitigation Plan Completion

Milestone 1: Configure ServiceDesk to send emails to [redacted] SMEs

File 1, "*RFC2017017546 Certification Package*", Milestone 1, Page 2, does show an example of task notification as indicated by milestone 1.

Milestone # 1 Completion Verified.

Milestone 2: Deep Dive of the change control application used in [redacted]

File 1, "RFC2017017546 *Certification Package*", Milestone 2, Pages 2 through 24, shows the meeting agenda, attendees list, and material covered during this meeting to "deep dive" the entity change control process.

Milestone # 2 Completion verified.

Milestone 3: Assets in compliance to all applicable requirements

File 2, "*Milestone 3*", Pages 2 through 134, show change controls tickets, explanations, and approvals from the entity [redacted] meetings for missed changes. This additional information provides clarity that was missing from the last submission proving that the entity is utilizing a change control program.

Milestone # 3 Completion Verified.

Milestone 4: Process Documentation

File 3, "*Milestone 4*", Pages 1 through 18, show the procedure that was requested in lieu of the process workflow submission. This procedures defines the roles and responsibilities that was missing from the previous submission.

Milestone # 4 Completion verified.

Milestone 5: [redacted] update

File 4, "*Milestone 5*", Pages 1 through 68, provides more detail into the how older than 30 days old change controls are tracked and escalated. The entity has implemented controls in order to add weekly review meetings and escalation in order to clear changes off the books that are approaching 30 days. If changes are to exceed 30 days, then the changes are to be submitted in multiple tickets in order to make them a more manageable size.

Milestone # 5 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: [redacted]

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-010-2
Requirement: CIP-010-2 R1.
Date Submitted: [redacted]
Has this violation previously been reported or discovered?: No

Entity Information:

Joint Registration Organization (JRO) ID:
Coordinated Functional Registration (CFR) ID:
Contact Name: [redacted]
Contact Phone: [redacted]
Contact Email: [redacted]

Violation:

Violation Start Date: June 07, 2017 **Changed to July 1, 2016**
End/Expected End Date:
Reliability Functions: [redacted]
Is Possible Violation still occurring?: No
Number of Instances: 1
Has this Possible Violation been reported to other Regions?: No
Which Regions:
Date Reported to Regions:

Detailed Description and Cause of Possible Violation: Detailed Description: On 4/19/17, while collecting evidence to support [redacted] CIP [redacted] RFI response on CIP010 R1, the [redacted] discovered an asset, [redacted] that is categorized as a PCA, without a documented baseline configuration and all other requirements applicable to a PCA. The asset ID [redacted] is located at IT [redacted] and [redacted] a [redacted] Rating Criteria (IRC) site. An extent of condition review found a second [redacted] asset CA [redacted] located in the [redacted] also without a baseline configuration. The [redacted] assets were implemented in production as part of CIP Versions 3 or before. Baseline configuration was not required in CIP versions prior to CIP Version 5 (CIPv5). As part of CIPv5 migration (7/1/16 Go-Live, [redacted] IRC), the [redacted] assets were not added to the CIP-007 and CIP-010 programs.

Root Cause of Possible Violation: Several root causes led to this omission. [redacted] asset owners were accountable for bringing their assets into CIPv5 compliance. Assets were assigned to specific [redacted] groups (i.e., Information Technology vs. [redacted] based on asset ownership applicability. In addition, 100% asset validation was not performed by every [redacted] for all assets they owned. As a result, the [redacted] owner accountable for these two [redacted] assets missed them as "in scope" requiring

baseline configurations.

The process for change control was implemented as part of CIPv5 migration for including initial or changes to baseline configuration. Since no changes occurred to these assets as part of CIPv5 migration, they were not processed through where review for asset baseline configuration would have been required.

The CIP program was implemented to ensure on-going CIP compliance. The program triggers and tracks completion of baselining, patching and other routine compliance activities. However, it did not include the as "in scope", so these PCA continued to be missed for applicable requirements and for evidence of protection that is in place.

The Root Cause of this Self Report is the CIPv5 migration process. Pre-specifications for this process failed to ensure that clear roles and responsibilities regarding asset "ownership" for inter- asset assessments for CIP compliance (i.e., which assets are required for Baseline) were fully understood and implemented.

How was the violation discovered? Identified 4/19/17, while collecting evidence to suppor CIP RFI . After 4/19/2017, during investigation, it was discovered that NERC BCS List CA assets do not have a baseline configuration.

Timeline:
1/1/10 Initial CA ID installed at IT as part of CIP Version 1 - 3. Baseline configuration was not required.
6/1/16 Business unit (asset owners were accountable for bringing their assets into CIPv5 compliance. The owner accountable for these 2 assets did not identify as "in scope".
7/1/16 CIPv5 Go-Live, assets. CA ID located at IT and CA located in the added to BCS List, but not identified for determination of baseline configuration and applicable PCA requirements.
7/2/16 program was implemented to ensure CIP compliance. Program manages triggers and tracks completion of baselining, patching and other routine compliance activities. However, it did not include the as "in scope," so these PCA continued to be missed for applicable requirements and for evidence of protection that is in place.
4/19/17 While collecting evidence to support CIP RFI , it was discovered that a PCA, did not have a baseline configuration. After 4/19/2017, during extent of condition investigation, a second missed asset at was identified.
4/24/17 (and performed to define root cause and mitigating activities for Self-Report.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: CIP-007 and CIP-010 programs, procedures, instructions and training (SWIs, Job Aids, on-boarding training, etc.), and current asset lists (i.e., Baseline, etc.) will be reviewed and modified as needed to ensure that pre-specifications include clear roles and responsibilities regarding asset "ownership" for inter- asset assessments for CIP compliance (i.e., which assets are required for Baseline) are fully understood and any gaps are remediated and implemented.
Mitigating Activities:
1. CIP-007 and CIP-010 programs, related controls, software, and

artifacts (procedures, SWIs, etc.), will be updated to ensure all BCS List assets (all Cyber Asset Classifications), are part of Baseline as needed.
2. Review current BCS List assets and confirm all are in Baseline as needed; if not mitigate to add them to Baseline.
3. CIP programs for subject matter expert (SME) Onboarding, CIP [redacted] will be reviewed to include guidance regarding [redacted] to define which Standards are applicable to which assets. This will also enhance accuracy of inter-[redacted] asset assessments (i.e., ensure assets are added to Baseline) when the asset is owned by one [redacted] group but located as another [redacted] stakeholder physical location (i.e., Information Technology vs. [redacted]
4. BCS List asset Walk Down procedures (Top-Down & Bottom-Up, physical & electronic) will be reviewed for proper controls to ensure all assets are accounted for in Baseline.
Preventive Measures:
1. The two [redacted] have been added to baseline configurations and to the CIP [redacted] program.
2. The CIP [redacted] program triggers and tracks completion of baselining, patching and other routine compliance activities.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Minimal

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: The potential impact of this violation if exploited, is noted to be Low VSL because failure to apply CIP-010 R1 baseline configuration controls to the [redacted] and the resulting failure of CIP-007 related controls (patching, etc.) may indirectly compromise the accuracy of [redacted] pro-active alert data. This might lead to a failure to identify real security events that could allow an internal or external threat to carry out malicious activities undetected.
The actual impact to the BPS is deemed to be Lower VSL because the assets are within an ESP and access controlled to limited and trained SMEs only. In addition, the availability of the services that relied on the affected assets was not impacted at any time during this violation or immediately afterwards.

Risk Assessment of Impact to BPS: Assets are within an ESP and access controlled to limited and trained SMEs only. In addition, the availability of the services that relied on the affected assets was not impacted at any time during this violation or immediately afterwards. Assets are within an ESP and access controlled to limited and trained SMEs only. In addition, the availability of the services that relied on the affected assets was not impacted at any time during this violation or immediately afterwards.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents

Self Report

From	Document Name	Description	Size in Bytes
No Documents			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code: RFCMIT013013

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017017765	CIP-010-2 R1.	

Mitigation Plan Submitted On: [redacted]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: June 30, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

(1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
(2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
(3) The cause of the Alleged or Confirmed Violation(s).
(4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
(5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
(6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
(7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
(8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
(9) Any other information deemed necessary or appropriate.
(10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
(11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

• The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.

• This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.

• If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.

• Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.

• Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.

• The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [redacted]

NERC Compliance Registry ID: [redacted]

Address: [redacted]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [redacted]

Title: [redacted]

Email: [redacted]

Phone: [redacted]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017017765	06/07/2017	CIP-010-2 R1.
Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

Brief Description: (What happened?)
On 4/19/17, while collecting evidence to support [redacted] CIP [redacted] RFI response on CIP010 R1, the [redacted] discovered an asset, [redacted] that is categorized as a PCA, without a documented baseline configuration and all other requirements applicable to a PCA. The asset CA [redacted] is located at IT [redacted] a [redacted] Rating Criteria (IRC) site. An extent of condition review found a second asset CA [redacted] located in the [redacted] IRC [redacted] also without a baseline configuration. The [redacted] assets were implemented in production as part of CIP Versions 3 or before. Baseline configuration was not required in CIP versions prior to CIP Version 5 (CIPv5). As part of CIPv5 migration (7/1/16 Go-Live, [redacted] IRC), the [redacted] assets were not added to the CIP-007 and CIP 010 programs.

Cause: (what caused the violation?)
Baseline configurations were not established for two [redacted]

Results of the RCA: (What is the root cause?)
The CIPv5 migration process failed to ensure that all assets required to have a baseline were 100% validated and implemented during the CIPv5 implementation project.

Relevant information regarding the identification of the violation(s):

While collecting evidence to support [redacted] CIP [redacted] RFI, the [redacted] discovered that two [redacted] did not have baseline configurations.

The [redacted] assets were implemented in production in the CIP v3 timeframe and baseline configuration was not required in CIP versions prior to CIP Version 5 (CIPv5). A process failure during the CIPv5 migration failed to identify the [redacted] as assets requiring baselines (7/1/16 Go-Live, [redacted] IRC) and hence the [redacted] assets were not added to the CIP-007 and CIP-010 programs. Additionally, a 100% validation was not performed on the final CIPv5 list to identify any assets that may be missing the requirements outlined in CIP-007 and CIP-010.

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

1. Bring both devices into or confirm, and document compliance with 14 NERC CIP requirements
1.1. CIP-005-05 R 1: Electronic Security Perimeter
1.2. CIP-006-06 R 1: Physical Security Plan
1.3. CIP-006-06 R 2: Visitor Control Program
1.4. CIP-007-06 R 1: Ports and Services
1.5. CIP-007-06 R 2: Security Patch Management
1.6. CIP-007-06 R 3: Malicious Code Prevention
1.7. CIP-007-06 R 4: Security Event Monitoring
1.8. CIP-007-06 R 5: System Access Controls
1.9. CIP-010-02 R 1: Configuration Change Management
1.10. CIP-010-02 R 2: Configuration Monitoring
1.11. CIP-010-02 R 3: Vulnerability Assessments
1.12. CIP-010-02 R 4: Transient Cyber Assets and Removable Media
1.13. CIP-011-02 R 1: Information Protection
1.14. CIP-011-02 R 2: BES Cyber Asset Reuse and Disposal

2. Update the [redacted] to include [redacted] assets. This also ensures that required NERC CIP tasks are completed and reviewed on established intervals.

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: June 30, 2017

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
1. Complete evidence of compliance	Bring both devices into or confirm, and document compliance with 14 NERC CIP requirements	06/30/2017	06/30/2017		No
2. Update [redacted] Program	Update the [redacted] to include [redacted] assets	06/30/2017	06/29/2017		No

Additional Relevant Information

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

(i) Risk is unauthorized access to [redacted] could be used to identify or mask system vulnerabilities
(ii) NA. Mitigation Plan has been implemented.

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

All protected cyber assets will be baselined and will be compliant with applicable requirements.

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.

2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.

3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

[redacted] Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: [redacted]

Title: [redacted]

[redacted]

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

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request 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)

Registered Entity Name: [redacted]
NERC Registry ID: [redacted]
NERC Violation ID(s): RFC2017017765
Mitigated Standard Requirement(s): CIP-010-2 R1.
Scheduled Completion as per Accepted Mitigation Plan: June 30, 2017
Date Mitigation Plan completed: June 30, 2017
RF Notified of Completion on Date: [redacted]
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017765 Certification Package.zip	File "RFC2017017765 Certification Package.zip" contains the cover page for the whole package and supporting documentation for each milestone.	3,184,074

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Mitigation Plan Verification for RFC2017017765

[redacted] ([redacted])

Standard/Requirement: CIP-010-2 R1

NERC Mitigation Plan ID: RFCMIT013013

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
[redacted]	[redacted]	[redacted]		[redacted]	06/30/17

Description of Issue

Baseline configurations were not established for two [redacted]

On 4/19/17, while collecting evidence to support [redacted] CIP [redacted] RFI response on CIP010 R1, the [redacted] ([redacted] [redacted] ([redacted] discovered an asset, [redacted] that is categorized as a PCA, without a documented baseline configuration and all other requirements applicable to a PCA. The asset CA [redacted] is located at IT [redacted] ([redacted] [redacted] a [redacted] Rating Criteria (IRC) site. An extent of condition review found a second [redacted] asset CA [redacted] located in the [redacted] IRC [redacted] ([redacted] also without a baseline configuration. The [redacted] assets were implemented in production as part of CIP Versions 3 or before. Baseline configuration was not required in CIP versions prior to CIP Version 5 (CIPv5). As part of CIPv5 migration (7/1/16 Go-Live, [redacted] IRC), the [redacted] assets were not added to the CIP-007 and CIP 010 programs.

.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017017765 Certification Package	CIP-010-2 R1

Verification of Mitigation Plan Completion

Milestone 1: Complete evidence of compliance.

File 1, "*RFC2017017765 Certification Package*", Milestone 1 Submit this document describes and/or demonstrates what was put in place to demonstrate the 2 [redacted] scanners are in compliance for the 14 NERC CIP standard/requirements for PCAs.

The submitted evidence included the recently developed baseline (page 3 and 38) for the [redacted] scanners.

The Malicious Software Prevention methods is stated to be Hardening (Page 37).

The 14 standards/requirements are listed below:

- 1.1. CIP-005-05 R 1: Electronic Security Perimeter (Page 20)
- 1.2. CIP-006-06 R 1: Physical Security Plan (Page 20)
- 1.3. CIP-006-06 R 2: Visitor Control Program (Page 20)
- 1.4. CIP-007-06 R 1: Ports and Services (Page 20)
- 1.5. CIP-007-06 R 2: Security Patch Management (Page 20)
- 1.6. CIP-007-06 R 3: Malicious Code Prevention (Page 37)
- 1.7. CIP-007-06 R 4: Security Event Monitoring (Page 21)
- 1.8. CIP-007-06 R 5: System Access Controls (Page 20)
- 1.9. CIP-010-02 R 1: Configuration Change Management (Page 31 and 38)
- 1.10. CIP-010-02 R 2: Configuration Monitoring (Page 32)
- 1.11. CIP-010-02 R 3: Vulnerability Assessments (Page 32)
- 1.12. CIP-010-02 R 4: Transient Cyber Assets and Removable Media (Page 6)

- 1.13. CIP-011-02 R 1: Information Protection (Page 9)
- 1.14. CIP-011-02 R 2: BES Cyber Asset Reuse and Disposal (Page 6)

Milestone # 1 Completion verified.

Milestone 2: Update [redacted]

File 1, *RFC2017017765 Certification Package*", Milestone 2 Submit Page 2, Email from [redacted] stating the [redacted] are in compliance with the Standards/requirements and the [redacted] activities are beginning.

Page 3, is the [redacted] tab on the [redacted] spreadsheet. The spreadsheet shows the CIP requirements for the [redacted] devices for the [redacted]

Milestone # 2 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: [redacted]

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-010-2
Requirement: CIP-010-2 R1.
Date Submitted: [redacted]
Has this violation previously been reported or discovered?: No

Entity Information:

Joint Registration Organization (JRO) ID:
Coordinated Functional Registration (CFR) ID:
Contact Name: [redacted]
Contact Phone: [redacted]
Contact Email: [redacted]

Violation:

Violation Start Date: June 23, 2017 **Changed to July 1, 2016**
End/Expected End Date:
Reliability Functions: [redacted]
Is Possible Violation still occurring?: No
Number of Instances: 1
Has this Possible Violation been reported to other Regions?: No
Which Regions:
Date Reported to Regions:

Detailed Description and Cause of Possible Violation: On 5/2/2017, while collecting data in response to ReliabilityFirst ([redacted] it was discovered that [redacted] (a [redacted] BES cyber system) was not documenting the results of required cyber security controls testing when performing non-routine configuration changes. These changes were completed outside of the documented routine patching process. The software changes completed since go live and that do not have supporting CIP-010 R1 P1.4.3 controls documentation are as follows:

Software Installed Updated Assets Affected	Change Order	Date Baseline Was
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	

4

Self Report

SMEs verified that security controls for each asset are still active and in place. No adverse impact has been realized since installation of above noted configuration changes. Each software is in baseline of respective assets. Current patch levels were maintained on these assets during the period.

*Root Cause of Possible Violation:
Identified root cause is lack of a Standard Work Instruction (SWI) at the SME level specifying roles and responsibilities for configuration change management, including documenting the result of the cyber security controls testing for non-routine configuration changes.

*How was the violation discovered?
Violation was discovered while gathering evidence for a request for information (RFI) during the

*Timeline:
1. July 1, 2016 - The requirement to identify cyber security controls that could be impacted by a configuration change, then verify no adverse effect after the change is implemented, and then document this action, came into effect.
2. May 2, 2017 - notified of the Potential Non-Compliance (PNC) caused by the lack of documentation of this process.
3. June 9, 2017 - An (was conducted to determine root cause and evaluate solutions.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Mitigating:
A communication via e-mail will be sent to all NERC SMEs reminding them of the requirement to document non-routine configuration change management.

Preventive Measures:
technical staff will develop a Configuration Change Management Standard Work Instruction (SWI), directed to the point of activity for the SMEs performing CIP-010 R1 P1.4 tasks.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS:

The Potential Impact to the BES is severe because Baseline Configuration Program (a high level program document) delineates the requirements in CIP-010 R1 P1.4 including "document the results of the verification." However, this procedure was not followed.

The actual impact to the BES is minimal because the SMEs verified that appropriate controls were in place.

Risk Assessment of Impact to BPS:

identifies that that potential impact to the BES is low. has not identified any negative impact to its Bulk Electric System assets as a result of this potential violation.

Self Report

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code: RFCMIT013022-1

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
RFC2017017840	CIP-010-2 R1.	

Mitigation Plan Submitted On: [redacted]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: September 08, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

(1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
(2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
(3) The cause of the Alleged or Confirmed Violation(s).
(4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
(5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
(6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
(7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
(8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
(9) Any other information deemed necessary or appropriate.
(10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
(11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

• The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.

• This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.

• If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.

• Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.

• Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.

• The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [redacted]

NERC Compliance Registry ID: [redacted]

Address: [redacted]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [redacted]

Title: [redacted]

Email: [redacted]

Phone: [redacted]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017017840	07/01/2016	CIP-010-2 R1.
Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

On 5/2/2017, while collecting data in response to ReliabilityFirst ([redacted] it was discovered that [redacted] (a [redacted] BES cyber system) was not documenting the results of required cyber security controls testing when performing non-routine configuration changes. These changes were completed outside of the documented routine patching process. The software changes completed since go live and that do not have supporting CIP-010 R1 P1.4.3 controls documentation are as follows:

Software Installed | Change Order Date Baseline Was Updated | Assets Affected

[redacted]

SMEs verified that security controls for each asset are still active and in place. No adverse impact has been realized since installation of above noted configuration changes. Each software is in baseline of respective assets. Current patch levels were maintained on these assets during the period.

Looking at the table above, a software was installed only 7 times since 7/1/2016 whereas patching is every month. These change orders were missed because of lack of template to perform testing of CIP005 and CIP007 controls. [redacted] developed the template on 06/21/2017 and a communication will be sent out to SMEs. An email explaining the template and the requirement to use it will be sent on 8/7/2017. By August 30, a requirement to complete the template will be added as a control to the [redacted] ([redacted] process when a SME changes the baseline of a NERC CIP asset.

Root Cause of Possible Violation:

Identified root cause is lack of a Standard Work Instruction (SWI) at the SME level specifying roles and responsibilities for configuration change management, including documenting the result of the cyber security controls testing for non-routine configuration changes.

How was the violation discovered?

Violation was discovered while gathering evidence for a request for information (RFI) during the [redacted]

Timeline:

July 1, 2016 - The requirement to identify cyber security controls that could be impacted by a configuration change, then verify no adverse effect after the change is implemented, and then documented this action, came into effect.

May 2, 2017 - [redacted] notified of the Potential Non-Compliance (PNC) caused by the lack of documentation of this process.

June 09, 2017 - An [redacted] ([redacted] was conducted to determine root cause and evaluate solutions.

What is the violation?

[redacted] was not documenting the results of required cyber security controls testing when performing non-routine configuration changes.

Relevant information regarding the identification of the violation(s):

Violation was discovered while gathering evidence for a request for information (RFI) during the [redacted]

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

Milestone 1: The intended outcome is to use a testing template as a control to document CIP-005 and CIP-007 changes. The evidence will show the testing template created.
Milestone 2: The intended outcome is to verify security controls for each asset are still active and in place. The evidence will show the completion of the Vulnerability Assessment and the results of its findings. If any discrepancies, they will be corrected.
Milestone 3: To immediately correct and for reduction of interim risk [redacted] has communicated an email to remind Asset Owners/SMEs to, always save evidence of verified cyber security controls after every change. Some business units were saving this evidence only after patching. The milestone completion evidence is the email distributed email reminder.
Milestone 4: The intended outcome is communicatee the new developed SWI to Subject Mater Experts (SMEs) in staff meeting. This will assure SMEs are aware of the new developed SWI going to be enforce able. The evidence will show a meeting agenda, attended sheet and brief summer on what was discussed with SMEs.

Milestone 5: The intended outcome is to ensure documentation of the results of configuration changes. [redacted] will develop a Standard Work Instruction (SWI) directed to the point of activity for the SMEs performing CIP-10 R1 P1.4. The SWI will provide guidance to how and when to document non-routine configuration changes. The milestone completion evidence is the issued SWI.

Milestone 6: The intended outcome is communicate the testing template to all SMEs. This will assure SMEs are aware of the developed template. The evidence will show the developed new template.

Milestone 7: The intended outcome is to add the testing template as requirement to the [redacted] process and communicate that to the SMEs as well. The evidence will show the added requirement to the [redacted] process and an email communication to the SMEs.

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: September 08, 2017

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Developed testing template	The testing template is to document CIP-005 and CIP-007 changes. This will verify that the required documentation is completed.	06/21/2017	06/21/2017		No
Immediate	To immediately	06/30/2017	06/30/2017		No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Communication across Business Units ([redacted]	correct the problem an email has been sent to all NERC SMEs reminding them of the requirement to document non-routine configuration change.				
Verification of Security Controls for Assets	Verify that security controls (CIP005 and CIP007) for each asset are still active and in place.	07/13/2017	07/13/2017		No
Communicate developed (SWI)	Communicate the developed Configuration Change Management Standard Work Instruction (SWI) in staff meeting.	08/02/2017	08/02/2017		No
Develop a Security Controls Validation SWI	Develop a Configuration Change Management Standard Work Instruction (SWI), directed to the point of activity for the SMEs performing CIP-010 R1 P1.4 tasks. .	08/07/2017	08/07/2017		No
Communicatee testing template	A communication will be sent out that a testing template directed to the point of activity for the SMEs performing CIP-010 R1 P1.4 tasks.	08/08/2017	08/08/2017		No
Adding the testing Template to [redacted]	A requirement to complete the testing template will be added as a control to the [redacted] process.	09/08/2017			No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
	The update will be communicated to all the SMEs.				

Additional Relevant Information

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

The Potential Impact to the BES is severe because [redacted] Baseline Configuration Program (a high-level program document) delineates the requirements in CIP-010 R1 P1.4 including "document the results of the verification." However, this procedure was not followed.

The actual impact to the BES is minimal because the SMEs verified that appropriate controls were in place.

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

By completion of the mitigation plan [redacted] will minimize similar issues from Occurring. Milestone 1 Milestone a testing template has been created to document CIP-005 and CIP-007 changes. This will verify that the required documentation is completed. Milestone 2 verifies security controls for each asset are still active and in place. Milestone 3 email sent to all NERC SMEs reminds them of the requirement to document non-routine configuration changes. Milestone 4 issues a Configuration Change Management Standard Work instruction (SWI), directed to the point of activity for the SMEs performing CIP-010 R1 P1.4 tasks. The SWI will provide guidance to how and when to document non-routine configuration changes. Milestone 6 a requirement to complete the testing template will be added as a control to the [redacted] process. The update will be communicated to all the SMEs.

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.

2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.

3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

[redacted] Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: [redacted]

Title: [redacted]

Authorized On: [redacted]

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request 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)

Registered Entity Name: [redacted]
NERC Registry ID: [redacted]
NERC Violation ID(s): RFC2017017840
Mitigated Standard Requirement(s): CIP-010-2 R1.
Scheduled Completion as per Accepted Mitigation Plan: September 08, 2017
Date Mitigation Plan completed: August 31, 2017
RF Notified of Completion on Date [redacted]
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017840 - Certification Package.zip	File "RFC2017017840 - Certification Package.zip" contains the cover page for the package. This file also contains the supporting evidence for each milestone.	5,074,849

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Mitigation Plan Verification for RFC2017017840

[redacted] ([redacted])

Standard/Requirement: CIP-010-2 R1

NERC Mitigation Plan ID: RFCMIT013022-1

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
[redacted]	[redacted]	[redacted]		[redacted]	08/31/17

Description of Issue

The [redacted] (a [redacted] BES cyber system) was not documenting the results of required cyber security controls testing when performing non-routine configuration changes. These changes were completed outside of the documented routine patching process.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017017840 Certification Package	CIP-010-2 R1

Verification of Mitigation Plan Completion

Milestone 1: Developed Testing template.

File 1, *"RFC2017017840 Certification Package"*, Milestone 1-Submit, Pages 1 through 3, show the testing template as mentioned by this milestone. This template tests against CIP-005 and CIP-007 security controls prior to implementation of a change.

Proposed Completion Date: June 21, 2017

[redacted]

Milestone 5: Develop a Security Controls Validation SWI.

File 1, *"RFC2017017840 Certification Package",* Milestone 5-submit, Pages 1 through 11, show the standard work instruction (SWI) as applicable to this milestone. It also provides email threads advising subject matter experts to complete the new version instead of past versions.

Proposed Completion Date: August 7, 2017

Actual Completion Date: August 3, 2017

Milestone # 5 Completion verified.

Milestone 6: Communicate testing template.

File 1, *"RFC2017017840 Certification Package",* Milestone6- submit, Pages 1 and 2, is the email communication directing subject matter experts to the new SWI template and that they are to use it moving forward.

Proposed Completion Date: August 8, 2017

Actual Completion Date: August 8, 2017

Milestone # 6 Completion verified.

Milestone 7: Adding the testing Template to [redacted]

File 1, *"RFC2017017840 Certification Package",* Milestone7- submit, Pages 1 through 68, show the procedure in which the testing template was added to the [redacted]. Page 68 also shows the revision history that describes this document change.

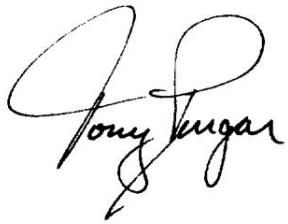
Proposed Completion Date: September 8, 2017

Actual Completion Date: August 29, 2017

Milestone # 7 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: [redacted]



Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-010-2
Requirement: CIP-010-2 R1.
Date Submitted: September 05, 2017
Has this violation previously been reported or discovered?: No

Entity Information:

Joint Registration Organization (JRO) ID:
Coordinated Functional Registration (CFR) ID:
Contact Name: [redacted]
Contact Phone: [redacted]
Contact Email: [redacted]

Violation:

Violation Start Date: July 20, 2017
End/Expected End Date:
Reliability Functions: [redacted]
Is Possible Violation still occurring?: No
Number of Instances: 1
Has this Possible Violation been reported to other Regions?: No
Which Regions:
Date Reported to Regions:

Detailed Description and Cause of Possible Violation:

Current Process

[redacted] follows an established, documented Change management process for requesting, approving and executing changes to IT assets, including NERC CIP assets. Per this process, named [redacted] Change Management, a user is required to create a Change Order (CO) to perform an addition, deletion or modification to hardware, software or security settings. Depending upon the IT asset for which the CO is applicable, an approval process is triggered. For NERC CIP assets, Change Orders are categorized as Urgent, System Restore, Normal and Standard pre-approved orders, with each type requiring an approval from [redacted]) prior to execution.

Incident description

Between October to November of 2016, four non-NERC Change orders (CO # [redacted]) were created to install a system backup software, named [redacted] on all production servers. [redacted] was intended to replace the existing backup software, [redacted] throughout the organization. The initiative and CO's at the time were to include all allowable production assets.

An IT Server Engineer from the [redacted] group, responsible for the implementation of these CO, was aware of the established [redacted] change management process and recognized two of the listed server names on the CO to be NERC CIP. He therefore proceeded to exclude these servers from

Self Report

the original CO's and decided to create a specific NERC CIP change order for these PACS servers at a later point in time. As per [redacted] CIP-011 program, server name is not a BCSI and hence listing of server names on the CO was not recorded as a violation.

In December 2016, the work tasks of the four CO's were completed and the CO's were closed for execution. No 'work tasks' could therefore be performed against these CO's going forward.

On 07/19/2017, another member of the [redacted] team, ran a maintenance job monitoring report on production servers. The report revealed PACS servers that were still running [redacted] He assumed that per the original CO's, [redacted] should have replaced [redacted] on these servers. Without double checking the Change orders, which had since been edited and closed, he proceeded to install [redacted] on two of the PACS servers. He did not deactivate [redacted] from the servers, per the standard practice of letting a software run in parallel for two weeks once the replacement was in place. This engineer did not recognize the servers as NERC CIP assets when he installed the software [redacted] on them.

On 07/26/2017, an IT technical analyst from [redacted] Identity Access Management team completed a [redacted] installation on 4 PACS Servers and 16 Workstations based on an authorized Change order [redacted]. She then ran a [redacted] Scan to generate a configuration monitoring report as output. The report was meant to review the new baseline configuration since a new software ([redacted] [redacted] had been intentionally installed on the managed NERC CIP assets. In addition to [redacted] the report highlighted a new commercial software package ([redacted] on 2 of the 4 PACS servers and noted it as an exception to the baseline. The last configuration monitoring report that ran on 07/19/2017 had not listed this noncompliance.

To validate if [redacted] was an authorized software, she confirmed the software name in the internal [redacted] search engine named [redacted] and found a cancelled CO# [redacted] created by [redacted] from 8/18/2016. She reached out to the [redacted] team to determine the details of the noted exception. On 7/27/2017, she was informed that [redacted] is the replacement for [redacted] and that no valid CO could be found to authorize this change to production. This IT technical analyst thus reported a NERC CIP violation to [redacted] [redacted] ([redacted]

On 08/30/2017, a team meeting was held between the [redacted] and the [redacted] [redacted] team, to create a detailed plan to retroactively correct this error. The plan includes creating a retroactive NERC CIP Change order for approval by [redacted] [redacted] to install [redacted] on all PACS production servers post a successful test is completed in the development environment. Once the change order has been executed, the plan also requires collection of evidence indicating authorized changes to the baseline.

*What is the problem?
A new commercial software ([redacted] was installed on 2 PACS production servers without a valid Change Order to authorize this change to production.

The change modified the baseline. This has been recorded as a violation of CIP-010- R1 P1.2 - "Authorize & document changes that deviate from the existing baseline configuration".

*Root Cause of Possible Violation:
As per the [redacted] & [redacted] performed on 08/21/2017, the root cause was identified to be a Human Error in following the process.

The [redacted] team member did not have an authorized Change order before proceeding to install a new software on the production servers. He worked off an assumption and did not follow the documented process. Based on an interview with his Manager and subsequent discussion of the

Self Report

Manager with his team of [redacted] leads, this was determined to be a human performance error.

*How was the violation discovered?
On 07/26/2017, an IT technical analyst completed the [redacted] Implementation on [redacted] PACS Servers and [redacted] Workstations. She then ran a [redacted] Scan that generated a configuration monitoring report as output. Apart from the newly installed [redacted] the report highlighted a new commercial software on the PAC servers ([redacted] that was an exception to the baseline. The last configuration monitoring report that ran on 07/19/2017 did not have this noncompliance. The IT technical analyst researched a change order to support the change to baseline and could not find one. She hence reported a CIP10 violation.

*Explain how is it determined that the Noncompliance is related to documentation, performance, or both.

On examining the root causes listed above, it was determined that noncompliance is related to Human performance error in following the defined process of creating a change order, prior to updating a production NERC CIP asset.

*Timeline:
1. October & November 2016 - Four CO's were created to replace [redacted] software with [redacted] (We refer to these as Original CO's through the Self Report).
2. December 2016 - A Server Engineer modified the original CO's to remove NERC CIP assets.
3. December 2016 - [redacted] team executed work tasks per the original CO's. On completion of the assigned work tasks, these CO's were closed. No further work tasks could now be performed against these CO's.
4. 19 July 2017 - A member of the [redacted] team, who was unaware of the edits made to the original CO's, ran a Job monitoring report on production servers, and noted two PACS servers were not updated with the [redacted] software.
5. 20 July 2017 - This [redacted] team member installed [redacted] on two PACS servers.
6. 26 July 2017 - An IT Technical analyst within the Identity Access Management team installed an authorized software [redacted] client' and then ran a [redacted] Scan. The scan detected [redacted] software as an exception to the baseline software on the NERC CIP servers.
7. 27 July 2017 - She reached out to the [redacted] team to confirm whether [redacted] was an authorized software and if an approved CO was available to confirm the installation of this software on the PACS production servers. She was informed by the [redacted] team that no valid CO existed to authorize this change.
8. 28 July 2017 - This user from Identity Access Management team filed a NERC CIP violation with the [redacted]
9. 21 August 2017 - [redacted] conducted an [redacted] with all involved team members to discuss the sequence of events, the root cause analysis and mitigating controls for the reported noncompliance.
10. 30 August 2017 - [redacted] and [redacted] team proceeded to create a detailed plan to retroactively correct the noncompliance. The plan includes work tasks to create a retroactive NERC Change order to authorize the [redacted] software on PACS production servers (if not already installed) and update the baseline configuration.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Mitigating Activities:

1. To Counter the Human error in following the process:
a. Per a meeting scheduled on 08/30/2017 with the [redacted]

Manager, Human Resources Employee relation will serve a disciplinary action against the server engineer who did not follow the documented process.
b. The [redacted] team will submit a retroactive change order to authorize the [redacted] software on the PACS servers.
2. To reemphasize Training of the change control process to the [redacted] team:
a. There is an action item to re-train all Server Engineers who have access to NERC CIP assets on the [redacted] change control process.

Preventative Measures:

To augment and strengthen current process and communications, it was finalized that [redacted] Team will create a checklist, that would serve as a quick reference to the [redacted] Change management process for every [redacted] while performing an update to a production server. These checks would include, amongst others, a check to validate if an asset is NERC CIP and a check to ensure that a software is tested in the development environment prior to installation in production. This checklist will be communicated to all members of the [redacted] and [redacted] team.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Minimal

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: Actual Impact:
The commercial software ([redacted] installed on the production PACS servers, is a pre-approved [redacted] software, intended to replace the existing system backup software ([redacted] throughout the organization. Most non-NERC production servers, were already commissioned with [redacted] at the point this CIP violation was reported to the [redacted]

Additionally, the original software of [redacted] was still functional in parallel on the PACS servers and had not been decommissioned. No [redacted] failure had been reported on the [redacted] servers on which [redacted] was installed. Therefore, system restore and backup functionality were not exposed to risk by installation of [redacted] on the PACS servers.

[redacted] team confirmed that [redacted] had only been installed on [redacted] servers to confirm the extent of impact. [redacted] manually checked the [redacted] scans on all PACS servers for a period of 6 months, beginning January 2017 through July 2017 and found only two instances of [redacted] on the servers as of 08/25/2017. These instances matched the [redacted] scan reported on 07/26/2017 by the IT technical analyst. This extent testing confirmed that the impact was limited to the two reported installations of [redacted]

A retroactive Change order is planned for submission to the internal [redacted] Change Review Board to authorize [redacted] on the PACS servers, if not installed already. This process will ensure that vulnerability test results and change to authorized baseline in the production environment is documented as per the established process.

Potential Impact:

Potential impact of installing [redacted] software on production servers was discussed during the [redacted] However, since the software was pre-authorized for installation on [redacted] assets and had been deployed in development environment for non-NERC servers, this impact was analyzed as a [redacted]

Self Report

Risk Assessment of Impact to BPS:	Since it was a pre-approved commercial software for [redacted] and was planned for installation on NERC CIP assets over the year, the impact of the [redacted] installation on the PACS production servers without an authorized change ticket, posed a low impact to BES.
Additional Entity Comments:	CIP09 - Recovery procedure for PACS will be updated for changes in backup technology from [redacted] to [redacted]

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017018307	CIP-010-2 R1.	

Mitigation Plan Submitted On: October 02, 2017

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: November 06, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

(1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
(2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
(3) The cause of the Alleged or Confirmed Violation(s).
(4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
(5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
(6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
(7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
(8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
(9) Any other information deemed necessary or appropriate.
(10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
(11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

• The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.

• This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.

• If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.

• Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.

• Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.

• The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [redacted]

NERC Compliance Registry ID: [redacted]

Address: [redacted]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [redacted]

Title: [redacted]

Email: [redacted]

Phone: [redacted]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017018307	07/20/2017	CIP-010-2 R1.
Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

Brief Description: (What happened?)
Current Process
[redacted] follows an established, documented Change management process for requesting, approving and executing changes to IT assets, including NERC CIP assets. Per this process, named [redacted] Change Management, a user is required to create a Change Order (CO) to perform an addition, deletion or modification to hardware, software or security settings. Depending upon the IT asset for which the CO is applicable, an approval process is triggered. For NERC CIP assets, Change Orders are categorized as Urgent, System Restore, Normal and Standard pre-approved orders, with each type requiring an approval from [redacted]) prior to execution.

Incident description
Between October to November of 2016, [redacted] non-NERC Change orders ([redacted]) were created to install a system backup software, named [redacted] on all production servers. [redacted] was intended to replace the existing backup software, [redacted] throughout the organization. The initiative and CO's at the time were to include all allowable production assets.
An IT Server Engineer from the [redacted] group, responsible for the implementation of these CO, was aware of the established [redacted] change management process and recognized two of the listed server names on the CO to be NERC CIP. He therefore proceeded to exclude these servers from the original CO's. As per [redacted] CIP-011 program, server name is not a BCSI and hence listing of server names on the CO was not recorded as a violation.
In December 2016, the work tasks of the four CO's were completed and the CO's were closed for execution. No 'work tasks' could therefore be performed against these CO's going forward.
On 07/19/2017, another member of the [redacted] team, ran a maintenance job monitoring report on production servers. The report revealed PACS servers that were still running [redacted] He assumed that per the original CO's, [redacted] should have replaced [redacted] on these servers. Without double checking the Change orders, which had since been edited and closed, he proceeded to install [redacted] on two of the PACS servers. He did not deactivate [redacted] from the servers, per the standard practice of letting a software run in parallel for two weeks once the replacement was in place. This engineer did not recognize the servers as NERC CIP assets when he installed the software [redacted] on them.
On 07/26/2017, an IT technical analyst from [redacted] team completed a [redacted] installation on [redacted] PACS Servers and [redacted] Workstations based on an authorized Change order # [redacted]. She then ran a [redacted] Scan to generate a configuration monitoring report as output. The report was meant to review the new baseline configuration since a new software [redacted] had been intentionally installed on the managed NERC CIP assets. In addition to [redacted] the report highlighted a new commercial software package [redacted] on 2 of the 4 PACS servers and noted it as an exception to the baseline. The last configuration monitoring report that ran on 07/19/2017 had not listed this noncompliance.
To validate if [redacted] was an authorized software, she reached out to the [redacted] team. On 7/27/2017, she was informed that [redacted] is the replacement for [redacted] and that no valid CO could be found to authorize this change to production. This IT technical analyst thus reported a NERC CIP violation to [redacted]

Cause: (what caused the violation?)

Violation of CIP-010-2 R1. P1.2 was caused by installation of a commercial software [redacted] on 2

PACS servers without an authorized Change order, thus causing a deviation from the existing baseline configuration without a supporting authorization and required documentation.

Results of the [redacted]: (What is the root cause?)

As per the [redacted] & [redacted] performed on 08/21/2017, the root cause was identified to be a Human Error in following the process.
The [redacted] team member did not have an authorized Change order before proceeding to install a new software on the production servers. He worked off an assumption and did not follow the documented process. Based on an interview with his Manager, this was determined to be a human performance error and Employee Relations was updated to serve a disciplinary action.

Relevant information regarding the identification of the violation(s):

On 07/26/2017, an IT technical analyst completed the [redacted] Implementation to [redacted]. She then ran a [redacted] Scan that generated a configuration monitoring report as output. The report highlighted a new commercial software on the [redacted] ([redacted] that was an exception to the baseline. The last configuration monitoring report that ran on 07/19/2017 did not have this noncompliance. The IT technical analyst researched a change order to support the change to baseline and could not find one. She hence reported a CIP10 violation.

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

Milestone 1 - Serve a disciplinary action to the Employee to Counter the Human error in following the process
Human Resources Employee relation served a disciplinary action against the Server Engineer who did not follow the process on 09/14/2017. The employee was present along with his manager from [redacted] to discuss the details with HR.

Milestone 2 - Issue a retroactive Change order for authorization of [redacted] on [redacted]
A change order was created as a retroactive NERC CIP Change orders for approval by [redacted] to install [redacted] on all [redacted] servers post a successful test is completed in the development environment. Once the change order has been executed, the IT analyst will collect evidence indicating authorized changes to the baseline.

Milestone 3 - Re-emphasize Training of the change control process to the [redacted] team
This includes identifying resources in [redacted] team that are authorized to work on NERC CIP assets and delivering the training on the existing change control process and protocols before 10/31/2017.

Milestone 4 - Create a checklist as a reference to the Change control process
The checklist will serve as a quick aid for server engineers to reference the existing change control process and its key controls. The checklist will not add anything new to the process but will assist as a quick reference to the documented controls.

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: November 06, 2017

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
1. Serve a disciplinary action to the employee in [redacted] for not following the defined and documented change control	The employee is an experienced member of the [redacted] team, who is aware of the change control process and uses it repeatedly for update of IT asset in the production environment.	09/14/2017	09/14/2017		No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
	In this instance, the employee proceeded to update a production [redacted] without checking if a valid CO existed for the required task.				
2. Create a retroactive Change order to install [redacted] on the production [redacted] and get it approved by [redacted] with approp	Since [redacted] was installed on the [redacted] without an authorization from [redacted] it was imperative that [redacted] brought it to the attention of the [redacted] by creating a retroactive Change order. The change order needed to be identified as 'NERC-CIP' per the process and routed to the [redacted] with the appropriate explanation of the incident. The retroactive Change order have since been authorized to install and activate [redacted] on the [redacted], post a successful test and vulnerability assessments in the development environment. [redacted] was also subsequently decommissioned	10/10/2017			No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
	from the [redacted].				
3. Re-emphasize the change control procedures and protocols with the [redacted] team	[redacted] will work with the [redacted] managers to identify the team members authorized to work on NERC CIP assets and retrain them on the Change Control process.	10/31/2017			No
4. Create a checklist to serve as a quick reference to the existing Change Control process	The checklist will not contain any new information other than what already exists in the Change control documentation. It would simply create a reference to necessary steps that are mandatory checks to ensure compliance to NERC CIP related change orders.	11/06/2017			No

Additional Relevant Information

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

Identification of Risk : [redacted] has not identified any risk to the BES. The commercial software ([redacted] installed on the production [redacted], is a pre-approved [redacted] software, intended to replace the existing system backup software ([redacted] throughout the organization. Most non-NERC production servers, were already commissioned with [redacted] at the point this CIP violation was reported to the [redacted] [redacted] [redacted]

Additionally, the original software of [redacted] was still functional in parallel on the [redacted] and had not been decommissioned. No [redacted] failure had been reported on the [redacted] on which [redacted] was installed. Therefore, system restore and backup functionality were not exposed to risk by installation of [redacted] [redacted] on the [redacted].
[redacted] team confirmed that [redacted] had only been installed on [redacted] to confirm the extent of impact. [redacted] manually checked the [redacted] scans on all PACS servers for a period of 6 months, beginning January 2017 through July 2017 and found only two instances of [redacted] on the servers as of 08/25/2017. These instances matched the [redacted] scan reported on 07/26/2017 by the IT technical analyst. This extent testing confirmed that the impact was limited to the two reported installations of [redacted]

Assessment of Potential Impact :
Potential impact of installing [redacted] software on production servers was discussed during the [redacted] However, since the software was pre-authorized for installation on [redacted] assets and had been deployed in development environment for non-NERC servers, this impact was analyzed as a low impact.

Action proposed : These include the checklist for the [redacted] team to reference prior to administering any change order to a NERC CIP asset, apart from re-training of staff on the process.

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

In order to address future BES reliability risk [redacted] has taken several steps to both address the violation identified in this mitigation plan and to prevent possible reoccurrences of this violation. All [redacted] team members who are authorized to implement a NERC CIP asset change order, will be retrained on the documented [redacted] Change order process and the role of [redacted] [redacted] ([redacted] A checklist of all required checks that needs to be performed prior and during a change, would be created and circulated within the [redacted] [redacted] team. The checklist will highlight the controls from the existing [redacted] Change order process. To control the impact of this incident in particular, a retroactive change order will be created to authorize [redacted] on the [redacted] with an explanation to the [redacted]

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

Additional to the mitigation items, Recovery procedure for [redacted] will be updated for changes in backup technology from [redacted] to [redacted] and communicated to the SME's to be in compliant with CIP09.

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.

2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.

3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

[redacted] Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: [redacted]

Title: [redacted]

Authorized On: October 02, 2017

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request 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)

Registered Entity Name: [redacted]
NERC Registry ID: [redacted]
NERC Violation ID(s): RFC2017018307
Mitigated Standard Requirement(s): CIP-010-2 R1.
Scheduled Completion as per Accepted Mitigation Plan: November 06, 2017
Date Mitigation Plan completed: November 02, 2017
RF Notified of Completion on Date: November 06, 2017
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2018018307 Certification Package.zip	File RFC2018018307 Certification Package.zip contains the cover sheet for whole package and also the supporting evidence for each milestone.	31,231,282

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Mitigation Plan Verification for RFC2017018307

[redacted]

Standard/Requirement: CIP-010-2 R1

NERC Mitigation Plan ID: RFCMIT013267

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 09/05/17	10/02/17	10/27/17	11/07/2017	11/06/17	11/02/17

Description of Issue

Between October to November of 2016, four non-NERC change orders were created to install a system backup software, named [redacted] on all production servers. [redacted] was intended to replace the existing backup software, [redacted] throughout the organization. The initiative and change orders at the time were to include all allowable production assets.

An [redacted] from the [redacted] group, responsible for the implementation of these change orders, was aware of the established [redacted] change management process and recognized two of the listed server names on the change orders to be NERC CIP. He therefore proceeded to exclude these servers from the original change orders. As per [redacted] CIP- 011 program, server name is not a BCSI and hence listing of server names on the CO was not recorded as a violation.

In December 2016, the work tasks of the four change orders were completed and the change orders were closed for execution. No 'work tasks' could therefore be performed against these change orders going forward.

On 07/19/2017, another member of the [redacted] team, ran a maintenance job monitoring report on production servers. The report revealed PACS servers that were still running [redacted] He assumed that per the original change orders, [redacted] should have replaced [redacted]

on these servers. Without double checking the Change orders, which had since been edited and closed, he proceeded to install [redacted] on two of the [redacted]. He did not deactivate [redacted] from the servers, per the standard practice of letting a software run in parallel for two weeks once the replacement was in place. This engineer did not recognize the servers as NERC CIP assets when he installed the software [redacted] on them.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2018018307 Certification Package	CIP-010-2 R1
File 2	[redacted] additional evidence needed RFC2017018307 responses	CIP-010-2 R1

Verification of Mitigation Plan Completion

Milestone 1: Serve a disciplinary action to the employee in [redacted] for not following the defined and documented change control.

Proposed Completion Date: September 14, 2017

Actual Completion Date: September 14, 2017

File 1, "*RFC2018018307 Certification Package*", Milestone1- Submit Pages 1 through 3, provide email conversations in regards to the disciplinary action carried out.

Milestone # 1 Completion verified.

Milestone 2: Create a retroactive Change order to install [redacted] on the production PACS servers and get it approved by [redacted]

Proposed Completion Date: October 10, 2017

Actual Completion Date: September 11, 2017

File 1, "*RFC2018018307 Certification Package*", Milestone 2-Submit, Pages 1 through 26, shows the change control history associated with this milestone along with required approvals, communications, baseline updates, and port changes as required.

Milestone # 2 Completion verified.

Milestone 3: Re-emphasize the change control procedures and protocols with the [redacted] team.

Proposed Completion Date: October 31, 2017

Actual Completion Date: September 11, 2017

File 1, "*RFC2018018307 Certification Package*", Milestone 2-Submit, Pages 1 through 26, shows the change control history associated with this milestone along with required approvals, communications, baseline updates, and port changes as required.

Milestone # 3 Completion verified.

Milestone 4: Create a checklist to serve as quick reference to existing Change Control process.

Proposed Completion Date: November 6, 2017

Actual Completion Date: November 11, 2017

Via a teleconference on November 9, 2017, and File 1, "*RFC2018018307 Certification Package*", Milestone-Submit Pages 1 through 4, shows a checklist for the [redacted] team. During a teleconference, the entity elaborated that since the host will be rebooted into maintenance mode that a change request is not needed per their procedure.

Milestone # 4 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: November 28, 2017

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-010-2

Requirement: CIP-010-2 R1.

Date Submitted: April 25, 2018

Has this violation previously been reported or discovered?: No

Entity Information:

Joint Registration Organization (JRO) ID:

Coordinated Functional Registration (CFR) ID:

Contact Name: [redacted]

Contact Phone: [redacted]

Contact Email: [redacted]

Violation:

Violation Start Date: July 01, 2016

End/Expected End Date: September 28, 2018

Reliability Functions: [redacted]

Is Possible Violation still occurring?: No

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: Current Process: The [redacted] server is a log collection device configured to collect system, security, event, and application logs from both [redacted] and [redacted] BCAs. The system is made up of a front-end server to run the application and a backend server to manage the database.

The [redacted] system forwards logs to [redacted] a [redacted] tool. All log capture and forwarding is done in near real time. Working as an intermediator server, the [redacted] servers are critical to the proper function of the [redacted]

Incident Description: The [redacted] server have been in place since October, 2012. According to SME this has never been classified as a NERC asset. The servers were not identified as NERC Electronic Access Control or Monitoring System (EACMS) assets during the v6 implementation. The [redacted] servers were also not identified as NERC assets up to or during the recent [redacted] implementation. The [redacted] however, has been identified as a NERC asset since its implementation and is compliant with all applicable CIP requirements.

[redacted] is upgrading the [redacted] servers for an updated application, [redacted] The upgrade includes new equipment, redundancy, and functionality. It was during the planning phase of

this upgrade that a subject matter expert (SME) identified the planned [redacted] systems as Electronic Access Control or Monitoring System (EACMS) assets. It was subsequently identified that the current system, [redacted] should have been identified as the same.

The processes related to the upgrade project, and related discussions regarding the failure to previously identify the NERC assets, yielded additional information as well:

The [redacted] process, the architectural review of assets at [redacted] determined that architectural diagrams for the [redacted] implementation exist, but the upgraded [redacted] system architectural documents have not been developed.

The [redacted] servers is not currently maintained within a Physical Security Perimeter (PSP). The server is located within the [redacted]

*Current protections in place?

The assets are housed in a [redacted] that includes controls similar to a PSP. However, is not a designated PSP. Access is controlled and monitored on a 24/7/365 basis.

The asset currently resides in the [redacted] Physical access controls utilize electronic card readers and unescorted access is granted to only authorized SME's who work in the area on a regular basis. They are also subject to an extensive background check. This [redacted] is not a designated PSP.

Hardening of the [redacted] server is accomplished with [redacted] Antivirus, the [redacted] agent installed and reporting to [redacted] and vulnerability scans.

The asset is behind firewalls to further restrict electronic access and to reduce the attack vectors that potential nefarious groups or individuals can utilize.

There is no remote capability from these systems to the BES.

The [redacted] is monitored 24X7 by the [redacted]

What is the problem?

The [redacted] servers are critical to the proper function of the [redacted] an identified NERC asset. However, the [redacted] servers are not currently identified as NERC assets, no baseline, thus in violation of CIP010 R1.1.

*Root Cause of Possible Violation:

[redacted] did not have architectural diagrams to examine to identify intermediate assets, so the system was examined and the [redacted] was determined to have been identified as an EACMS assets in the NERC space per the [redacted] SME.

*How was the violation discovered?

The violation was discovered during the preliminary steps of a planned upgrade of the [redacted] server.

*Explain how is it determined that the Noncompliance is related to documentation, performance, or both.

The noncompliance is related to documentation because [redacted] lacks a requirement to create, maintain, and regularly review documented architectural diagrams. The documentation and periodic review process will identify all NERC assets.

Self Report

*Timeline:

10/19/2012 The [redacted] server was installed at [redacted]

7/1/2016 The CIP standards version 6 was implemented.

2/14/2018 The [redacted] ([redacted] was notified by a SME of a Potential Non Compliance with the CIP standards.

3/5/2018 [redacted] ([redacted] conducted.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Immediate Correcting Activities:

In an examination of how to mitigate this issue, no clear path was presented that can be implemented without causing interruptions to logging. It was determined that implementing the proposed upgrade is the best option to mitigate this issue. With the upgrade in place, [redacted] can run systems in parallel and move assets over one at a time and with no interruptions in logging or loss of data integrity. [redacted] is currently running a project to upgrade the [redacted] ([redacted] to [redacted] [redacted] [redacted] ([redacted] For this upgrade to take place, new hardware needs to be acquired. In addition to acquiring the new server hardware, a new PSP cabinet may also be need to be acquired for additional space.

Mitigating Activities:

[redacted] is doing the vulnerability scans on this server.

The application is restricted to only those SME's who need to use it. It is controlled by a password management that controls who has access to the application.

Logging and generating alerts for security events on the [redacted] server to look for suspicious activity has been implemented since at least July of 2016 so [redacted] is in compliance with CIP 007 R4.1, R4.2, and R4.3.

This machine is being monitored on the Corporate [redacted] environment instead of the NERC [redacted] environment.

Preventative Measures:

The [redacted] ([redacted] is [redacted] standard process for application teams to interface with Shared Infrastructure. All [redacted] projects, with or without an impact on NERC assets, go through a [redacted] review process. [redacted] is one of the gates where we should have identified the [redacted] server. The current [redacted] methodology does not distinguish between NERC or Non-NERC assets. This is a mitigation item from RFC2018019428.

The purpose of this milestone is to enhance the [redacted] review process to include the identification of NERC projects or projects that likely impact a NERC asset or system. If a NERC impact is identified, the review will be suspended until a NERC representative is invited to participate.

Enhance the project methodology to integrate NERC requirements into the build and implementation processes.

The [redacted] Group in [redacted] performs two critical functions in any IT project: The "Architecture Design Review" takes place in the design phase of a project. Technologies like virtual environments, hosting, and [redacted] server

are expected to be discussed in this process. The "Pre-Production Review" verifies that the implementation matches the agreed upon architectural design. Any gaps or deviations are investigated. [redacted] will develop a list of requirements that will be utilized by the [redacted] Group, on behalf of [redacted] during the Architecture Design Review and verified in the Pre-Production Review. This is a mitigation item from RFC2018019428.

In addition, [redacted] will be investigating to make sure that no other NERC assets are misidentified. This will be accomplished by using [redacted] rules to determine what event feeds from the ESPs are allowed. That information will be used to verify and identity any additional NERC assets.

Upgrade of [redacted] to [redacted] [redacted] ([redacted]
It was determined that implementing the proposed upgrade is the best option to mitigate this issue. With the upgrade in place, [redacted] can run systems in parallel and move assets over one at a time with no interruption in logging or loss of data integrity. [redacted] is currently running a project to upgrade the [redacted] ([redacted] to [redacted] [redacted] [redacted] ([redacted] For this upgrade to take place, new hardware needs to be acquired. In addition to acquiring the new server hardware, a new PSP cabinet may also be need to be acquired for additional storage space.

The purpose of this milestone is to show the [redacted] has migrated from the [redacted] ([redacted] to [redacted] [redacted] [redacted] ([redacted]

Once the upgrade to [redacted] [redacted] ([redacted] which is schedule to take place by August 31, 2018, is complete. The [redacted] will be added to the [redacted] program. The upgrade will include the architectural diagrams. Completion of this milestone directly addresses the root cause. To bring the [redacted] into compliance by implementing all applicable requirements in the [redacted]

Remove [redacted] server by September 28, 2018. This is currently a virtual machine.

Evidence of compliance with the following requirements will be provided:

CIP-002-5.1: Asset List
CIP-005-5, R1: Electronic Security Perimeter.
CIP-005-5, R2: Interactive Remote Access Management
CIP-006-6, R1.2: Physical Access Controls
CIP-006-6, R1.3: Physical Access Controls
CIP-006-6, R1.4: Monitoring for Unauthorized access
CIP-006-6, R1.5: Alarm or alert in response to unauthorized access
CIP-006-6, R1.8: Log entry of each individual with authorized unescorted physical access
CIP-006-6, R1.9: Retain physical access logs for ninety days
CIP-006-6, R2.1: Require continuous escorted access of visitors
CIP-006-6, R2.2: Require logging of visitor entry and exit
CIP-006-6, R2.3: Retain visitor logs for ninety days
CIP-007-6, R1.1: Ports and Services.
CIP-007-6, R2: Security Patch Management.
CIP-007-6, R3: Malicious Code Prevention.
CIP-007-6, R4: Security Event Monitoring.
CIP-007-6, R5: System Access Controls.
CIP-009-6, R1: Recovery Plan Specifications.
CIP-010-2, R1.1: Develop a baseline configuration

Self Report

Date Mitigating Activities Completed: September 28, 2018

Impact and Risk Assessment:

Potential Impact to BPS: Severe

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: The potential impact the BES could be High if there were no controls in place. The [redacted] contains BCSI information and if this information would be disclosed to a nefarious group or individual then the systems at [redacted] could be compromised greatly increasing the risk that the BES could be effected.

Actual Impact:

The actual impact to the BES would be low because of the controls that are currently in place to protect these assets.

The asset currently resides in the [redacted] Physical access controls utilize electronic card readers and unescorted access is granted to only authorized SME's who work in the area on a regular basis. They are also subject to an extensive background check.

Hardening of the [redacted] server is accomplished by [redacted] Antivirus. It has the [redacted] agent installed which means that events show up on [redacted] The server is being scanned by [redacted]

These asset is also behind firewalls for added protection and to reduce the attack vectors that potential nefarious groups or individuals can use to attack these assets.

There is no remote capability from these systems to the BES.

These assets are also under monitoring of PSP 24X7 in [redacted]

Risk Assessment of Impact to BPS: The risk of Impact to the BES has been identified as low. There is no remote capability from these systems to the BES. It is isolated from the BES by firewalls. These systems are also maintained in the [redacted] so access is limited to only SME's who have a need to access these systems.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
RFC2018019647	CIP-010-2 R1.	

Mitigation Plan Submitted On: June 01, 2018

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: September 28, 2018

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

(1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
(2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
(3) The cause of the Alleged or Confirmed Violation(s).
(4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
(5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
(6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
(7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
(8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
(9) Any other information deemed necessary or appropriate.
(10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
(11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

• The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.

• This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.

• If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.

• Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.

• Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.

• The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [redacted]

NERC Compliance Registry ID: [redacted]

Address: [redacted]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [redacted]

Title: [redacted]

Email: [redacted]

Phone: [redacted]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2018019647	07/01/2016	CIP-010-2 R1.
Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

C.1 This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID (if known) Date of Violation Requirement
RFC2018019647 7/1/2016 CIP-010-2 R1.1
Requirement Description:
Develop a baseline configuration, individually or by group, which shall include the following items:
1.1.1 Operating system(s) (including version) or firmware where no independent operating system exists;
1.1.2 Any commercially available or open-source application software (including version) intentionally installed;
1.1.3 Any custom software installed;
1.1.4 Any logical network accessible ports; and
1.1.5 Any security patches applied.

C.2 Brief summary including the cause of the violation(s) and mechanism in which it was identified above:

Current Process: The [redacted] ([redacted] server is a log collection device configured to collect system, security, event, and application logs from both [redacted] and [redacted] BCAs. The system is made up of a front-end server to run the application and a backend server to manage the database.

The [redacted] system forwards logs to [redacted] a [redacted] ([redacted] tool. All log capture and forwarding is done in near real-time. Working as an intermediator server, the [redacted] servers are critical to the proper function of the [redacted]

Incident Description: The [redacted] server have been in place since October, 2012. According to SME this has never been classified as a NERC asset. The servers were not identified as NERC Electronic Access Control or Monitoring System (EACMS) assets during the v6 implementation. The [redacted] servers were also not identified as NERC assets up to or during the recent [redacted] [redacted] implementation. The [redacted] however, has been identified as a NERC asset since its implementation and is compliant with all applicable CIP requirements.

[redacted] ([redacted] is upgrading the [redacted] servers for an updated application, [redacted] [redacted] ([redacted] The upgrade includes new equipment, redundancy, and functionality. It was during the planning phase of this upgrade that a subject matter expert (SME) identified the planned [redacted] systems as Electronic Access Control or Monitoring System (EACMS) assets. It was subsequently identified that the current system, [redacted] should have been identified as the same.

The processes related to the upgrade project, and related discussions regarding the failure to previously identify the NERC assets, yielded additional information as well:
The [redacted] ([redacted] process, the architectural review of assets at [redacted] determined that architectural diagrams for the [redacted] implementation exist, but the upgraded [redacted] system architectural documents have not been developed.
The [redacted] servers is not currently maintained within a Physical Security Perimeter (PSP). The server is located within the [redacted] [redacted] [redacted]

Current protections in place?

The assets are housed in a [redacted] that includes controls similar to a PSP. However, is not a designated PSP. Access is controlled and monitored on a 24/7/365 basis.
The asset currently resides in the [redacted] Physical access controls utilize electronic card readers and unescorted access is granted to only authorized SME's who work in the area on a regular basis. They are also subject to an extensive background check. This [redacted] is not a designated PSP.
Hardening of the [redacted] server is accomplished with [redacted] Antivirus, the [redacted] agent installed and reporting to [redacted] and vulnerability scans.
The asset is behind firewalls to further restrict electronic access and to reduce the attack vectors that potential nefarious groups or individuals can utilize.
There is no remote capability from these systems to the BES.
The [redacted] is monitored 24X7 by the [redacted]

Relevant information regarding the identification of the violation(s):

What is the problem?

The [redacted] servers are critical to the proper function of the [redacted] an identified NERC asset. However, the [redacted] servers are not currently identified as NERC assets, no baseline, thus in violation of CIP010 R1.1.
Root Cause of Possible Violation:

[redacted] did not have architectural diagrams to examine to identify intermediate assets, so the system was examined and the [redacted] was determined to have been identified as an EACMS assets in the NERC space per the [redacted] SME.

*How was the violation discovered?

The violation was discovered during the preliminary steps of a planned upgrade of the [redacted] server.

Explain how is it determined that the Noncompliance is related to documentation, performance, or both.

The noncompliance is related to documentation because [redacted] lacks a requirement to create, maintain, and regularly review documented architectural diagrams. The documentation and periodic review process will identify all NERC assets.

Timeline:
10/19/2012 - The [redacted] server was installed at [redacted]

7/1/2016 - The CIP standards version 6 was implemented.

2/14/2018 - The [redacted] was notified by a SME of a Potential Non Compliance with the CIP standards.

3/5/2018 - [redacted] conducted.

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

Milestone One: In addition, [redacted] will be investigating to make sure that that the only systems that were acting as log aggregators for CIP007 R4 compliance for NERC Cyber Assets were the [redacted] application, and database servers and the [redacted]). This will be accomplished by using [redacted] rules to determine what event feeds from the ESPs are allowed. That information will be used to verify and identity any additional NERC assets.

Purpose of this milestone is to understand the extent of condition on the servers that make up [redacted] solution only. The extent of condition for all the assets reporting to [redacted] was executed in milestone 2 of violation RFC2018019469.

Evidence: Documentation will be provided to support that the only systems that were acting as log aggregators for CIP007 R4 compliance for NERC Cyber Assets were the [redacted] application, and database servers and the [redacted]). Everything else identified as a log source was a NERC Cyber Asset that sends its logs directly to [redacted] without the need for log aggregation or a non-NERC Operational Technology (OT) asset.
Milestone Two: Update [redacted]
The [redacted] ([redacted] is [redacted] standard process for application teams to interface with Shared Infrastructure. All [redacted] projects, with or without an impact on NERC assets, go through a [redacted] review process. [redacted] is one of the gates where we should have identified the [redacted] servers. The current [redacted] methodology does not distinguish between NERC or Non-NERC assets.

The purpose of this milestone is to enhance the [redacted] review process to include the identification of NERC projects or projects that likely impact a NERC asset or system. If a NERC impact is identified, the review will be suspended until a NERC representative is invited to participate.

Evidence: An updated [redacted] process will be provided.

Milestone Three: Enhance the project methodology to integrate NERC requirements into the build and implementation processes.

The purpose of this milestone is to integrate NERC requirements into the build and implementation process for new projects affecting NERC assets.

The [redacted] in [redacted] performs two critical functions in any IT project: The "Architecture Design Review" takes place in the design phase of a project. Technologies like virtual environments, hosting, and [redacted] are expected to be discussed in this process. The "Pre-Production Review" verifies that the implementation matches the agreed upon architectural design. Any gaps or deviations are investigated. [redacted] will work with the [redacted], during the Architecture Design Review and verified in the Pre-Production Review.

Evidence: Updated documented processes for the Architecture Design Review and Pre-Production Review, each including use of the requirements list provided by [redacted] communicated to all impacted parties.

Milestone Four: Once the upgrade to [redacted] ([redacted] which is schedule to take place by August 31, 2018, is complete. The [redacted] will be added to the [redacted] program. The upgrade will include the architectural diagrams. Completion of this milestone directly addresses the root cause. To bring the [redacted] into compliance by implementing all applicable requirements in the [redacted]
The purpose of this milestone is to make sure the [redacted] ([redacted] is in compliance with NERC CIP requirements at the time of onboarding and added to the [redacted]

Evidence: Evidence of compliance with the following requirements will be provided:
CIP-002-5.1: Asset List

CIP-005-5, R1: Electronic Security Perimeter.
CIP-005-5, R2: Interactive Remote Access Management
CIP-006-6, R1.2: Physical Access Controls
CIP-006-6, R1.3: Physical Access Controls
CIP-006-6, R1.4: Monitoring for Unauthorized access
CIP-006-6, R1.5: Alarm or alert in response to unauthorized access
CIP-006-6, R1.8: Log entry of each individual with authorized unescorted physical access
CIP-006-6, R1.9: Retain physical access logs for ninety days
CIP-006-6, R2.1: Require continuous escorted access of visitors
CIP-006-6, R2.2: Require logging of visitor entry and exit
CIP-006-6, R2.3: Retain visitor logs for ninety days
CIP-007-6, R1.1: Ports and Services.
CIP-007-6, R2: Security Patch Management.
CIP-007-6, R3: Malicious Code Prevention.
CIP-007-6, R4: Security Event Monitoring.
CIP-007-6, R5: System Access Controls.
CIP-009-6, R1: Recovery Plan Specifications.
CIP-010-2, R1.1: Develop a baseline configuration

Milestone Five: Remove [redacted] server by September 28, 2018. This is currently a virtual machine.

The purpose of this milestone is to make sure that the decommissioned asset is removed from the network.

Evidence: A closed and successfully completed change order and a network/logical diagram showing [redacted] solution.

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: September 28, 2018

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Milestone 1: Extent of Condition	Purpose: [redacted] will be investigating to make sure that that the only systems that were acting as log aggregators for CIP007 R4 compliance for NERC Cyber Assets were the [redacted] application, and database servers and the [redacted]	04/13/2018	04/04/2018		No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
	[redacted] Evidence: Documentation will be provided to support that the only systems that were acting as log aggregators for CIP007 R4 compliance for NERC Cyber Assets were the [redacted] application, and database servers and the [redacted] Everything else identified as a log source was a NERC Cyber Asset that sends its logs directly to [redacted] without the need for log aggregation or a non-NERC Operational Technology (OT) asset.				
Milestone 2: Update [redacted]	Purpose: Enhance the [redacted] review process to include the identification of NERC projects or projects that likely impact a NERC asset or system. If a NERC impact is identified, the review will be suspended until a NERC representative is invited to participate. Evidence: An updated [redacted]	05/31/2018	05/30/2018		No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
	process will be provided.				
Milestone 3: Enhance the project methodology to integrate NERC requirements into the build and implementation processes.	Purpose: Update the architectural review processes, integrating the use of the NERC guidance. Evidence: Updated documented processes for the Architecture Design Review and Pre-Production Review, each including use of the requirements list provided by [redacted] communicated to all impacted parties.	06/28/2018			No
Milestone 4: Bring newly identified [redacted] ([redacted]) cyber assets into compliance.	Purpose: Bring identified [redacted] ([redacted]) into compliance and document. Evidence: Documentation will be provided to support compliance with applicable CIP requirements	09/28/2018			No
Milestone 5: Remove old [redacted] server.	Purpose: Remove [redacted] server. Evidence: A closed and successfully completed change order and a network/logical diagram showing [redacted] solution.	09/28/2018			No

Additional Relevant Information

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

All impacted teams are working in a state of heightened awareness to detect and identify projects that may have been similarly impacted. Communications have been sent to stakeholders and discussions have been initiated to identify and prevent not only this specific type of reoccurrence, but related events.

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

Updated [redacted] as per Milestone two and updated start and end phases of project management as noted in Milestone three are expected to prevent the reoccurrence of similar issues.

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.

2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.

3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

[redacted] Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: [redacted]

Title: [redacted]

Authorized On: June 01, 2018

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request 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)

Registered Entity Name: [redacted]
NERC Registry ID: [redacted]
NERC Violation ID(s): RFC2018019647
Mitigated Standard Requirement(s): CIP-010-2 R1.
Scheduled Completion as per Accepted Mitigation Plan: October 19, 2018
Date Mitigation Plan completed: October 16, 2018
RF Notified of Completion on Date: October 19, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2018019647_Certification Package_Cover Page.zip	This is the Certification Package for RFC2018019647.	31,279,270

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Mitigation Plan Verification for RFC2018019647

[redacted] ([redacted])

Standard/Requirement: CIP-010-2 R1

NERC Mitigation Plan ID: RFCMIT013784-1

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 04/25/18	06/01/18	06/06/18	06/21/18	10/19/18	10/18/18

Description of Issue

Mitigation Task RFC2018019647

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2018019647 Certification Package Cover Page	CIP-010-2 R1

Verification of Mitigation Plan Completion

Milestone 1: Extent of Condition.

Proposed Completion Date: April 13, 2018

Actual Completion Date: April 4, 2018

File 1, "*RFC2018019647 Certification Package Cover Page,*" Milestone 1 - Submit, Pages 2 through 5, contain [redacted] screengrabs showing that the [redacted] Database ([redacted] DB Server) and [redacted] systems

were the only systems providing log aggregation and event information. Additionally, the referenced document includes the systems' current and future architecture.

Milestone # 1 Completion verified.

Milestone 2: Update [redacted]

Proposed Completion Date: May 31, 2018

Actual Completion Date: May 30, 2018

File 1, "*RFC2018019647 Certification Package Cover Page*," Milestone 2 – Submit, Pages 2 through 5, show the updates made to the entity's [redacted] process, including the participation of a [redacted] representative in the process in order to help identify projects that have a NERC CIP impact and reduce project delays.

Milestone # 2 Completion verified.

Milestone 3: Enhance the project methodology to integrate NERC requirements into the build and implementation processes.

Proposed Completion Date: June 28, 2018

Actual Completion Date: May 30, 2018

File 1, "*RFC2018019647 Certification Package Cover Page*," Milestone 3 - Submit, Pages 2 through 46, show a documented NERC CIP Checklist, documented processes for the Architecture Design Review and Pre-Production Review (each including use of the NERC CIP Checklist), and confirmation that the updated processes were communicated to all affected parties.

Milestone # 3 Completion verified.

Milestone 4: Bring newly identified [redacted] cyber assets into compliance.

Proposed Completion Date: October 19, 2018[1]

Actual Completion Date: October 18, 2018

File 1, "*RFC2018019647 Certification Package Cover Page*," Milestone 4- Submit, Pages 2 through 457, show how the entity has brought the [redacted] cyber assets into compliance with all applicable CIP standards.

Milestone # 4 Completion verified.

Milestone 5: Remove old [redacted] server.

Proposed Completion Date: October 19, 2018

Actual Completion Date: October 16, 2018

File 1, "*RFC2018019647 Certification Package Cover Page*," Milestone 5 - Submit, Pages 2 through 21, show the approved change control tickets verifying the removal of the old [redacted] server assets and the implementation of the new [redacted]

Milestone # 5 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: November 19, 2018

Anthony Jablonski
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

[1] The original completion date for Milestones 4 and 5 was September 28, 2018; however, [redacted] requested an extension of time to complete said Milestones. ReliabilityFirst Corporation granted the request and extended the completion date for Milestones 4 and 5 to October 19, 2018.

Attachment 14

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

14.a The Entity's Self-Report (RFC2017017836);
14.b The Entity's Mitigation Plan designated as RFCMIT013048 submitted [redacted];
14.c The Entity's Certification of Mitigation Plan Completion dated [redacted];
14.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted];
14.e The Entity's Self-Report (RFC2017018498);
14.f The Entity's Mitigation Plan designated as RFCMIT013394-1 submitted [redacted];
14.g The Entity's Certification of Mitigation Plan Completion dated [redacted];
14.h ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted];
14.i The Entity's Self-Report (RFC2018019048);
14.j The Entity's Mitigation Plan designated as RFCMIT013546 submitted [redacted];
14.k The Entity's Certification of Mitigation Plan Completion dated [redacted];
14.l ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted]

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-010-2
Requirement: CIP-010-2 R3.
Date Submitted: [redacted]
Has this violation previously been reported or discovered?: No

Entity Information:

Joint Registration Organization (JRO) ID:
Coordinated Functional Registration (CFR) ID:
Contact Name: [redacted]
Contact Phone: [redacted]
Contact Email: [redacted]

Violation:

Violation Start Date: July 01, 2016
End/Expected End Date:
Reliability Functions: [redacted]
Is Possible Violation still occurring?: No
Number of Instances: 1
Has this Possible Violation been reported to other Regions?: No
Which Regions:
Date Reported to Regions:

Detailed Description and Cause of Possible Violation:

*Detailed Description:
On March 2017, during an internal Quality Assurance review it was discovered that [redacted] was routinely not performing an active vulnerability assessment prior to adding assets into the production environment. Assets added to the [redacted] a [redacted] production environment have not been actively scanned for vulnerability since 7/1/2016. Total assets added without performing a vulnerability assessment were [redacted]. Those assets included [redacted] management port devices, [redacted] servers, [redacted] data backup devices, [redacted] workstations, and [redacted] printer. Of the total of [redacted] assets, [redacted] management port devices were disabled and removed from production. The remaining [redacted] devices were added since July 1, 2016. This violates CIP010 R3.3 for applicable [redacted] BES cyber system.

*Root Cause of Possible Violation:
Formal procedures on how and when active vulnerability assessments should be performed were not established.
*How was the violation discovered?
Violation was discovered during an internal QA review performed early March 2017 and was confirmed while collecting data for [redacted] RFI.

*Timeline:
July 1, 2016 - Start of period in which vulnerability assessments were not performed prior to adding assets in production.
March, 2017 - [redacted] performs internal QA and

extent of condition on CIP007 requirements and identifies the omissions.
Mid-April - Response to RFI confirms previously identified omissions.
April 27, 2017 - [redacted] notified of the Potential Violation.
May 17, 2017 - An [redacted] ([redacted] was conducted.
May 2017 - Vulnerability assessment is performed on all assets types within the production environment, including all assets added from July 2016 to March 2017.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Mitigating:
Create Vulnerability Assessment Procedures describing how and when active vulnerability assessments should be performed as required in CIP-010 R3.3.
[redacted] will enforce the updates of Vulnerability Management and Assessment Program and new procedures across business units to help understand how and when CIP-010 R3.3 be executed.
Complete evidence of compliance (Action plan to remediate or mitigate the vulnerabilities identified) for CIP-010 R3.4.

Preventive Measures:
During May 2017, vulnerability assessment performed on all assets types within the production environment, including all assets added from July 2016 to March 2017.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: The actual impact is minimum because the assets are in an ESP, ports and services are monitored monthly, [redacted] monitors for successful and failed logons, number of personnel with access is limited, and the firewall rules allow only the required traffic.

Risk Assessment of Impact to BPS: [redacted] identifies that that potential impact to the BES is low because the vulnerability assessment on the production environment after the [redacted] showed no vulnerability. [redacted] has not identified any negative impacts to its Bulk Electric System assets as a result of this potential violation.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Self Report

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code: RFCMIT013048

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017017836	CIP-010-2 R3.	

Mitigation Plan Submitted On: [redacted]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: November 30, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

(1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
(2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
(3) The cause of the Alleged or Confirmed Violation(s).
(4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
(5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
(6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
(7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
(8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
(9) Any other information deemed necessary or appropriate.
(10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
(11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

• The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.

• This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.

• If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.

• Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.

• Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.

• The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [redacted]

NERC Compliance Registry ID: [redacted]

Address: [redacted]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [redacted]

Title: [redacted]

Email: [redacted]

Phone: [redacted]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017017836	07/01/2016	CIP-010-2 R3.
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 R3– Vulnerability Assessments.		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

In March 2017, during an internal Quality Assurance review it was discovered that [redacted] was routinely not performing an active vulnerability assessment prior to adding assets into the production environment. Assets added into a [redacted] production environment have not been actively scanned for vulnerability since 7/1/2016. This violates CIP010 R3 P3.3 for applicable [redacted] BES cyber system.

While the mitigating activities are being worked on, [redacted] team has verbally notified to inspect new change orders to ensure the execution of active vulnerability in addition to checking for baseline changes and port and services.

Cause of Possible Violation:

[redacted] process did not include process to assess "new" assets added to production.

Results of the RCA: (What is the root cause?)

[redacted] program "[redacted]" states that "Before a new asset is added to the [redacted] BES Cyber System, an active vulnerability assessment is performed.". However, no checks existed in change control ([redacted] procedure to verify that the active vulnerability assessment is performed. [redacted] change control process included checking for baseline changes and port and services. This gap resulted in the violation of CIP010 R3 P3.3.

Timeline:
July 1, 2016 - Start of period in which vulnerability assessments were not performed prior to adding assets in production.
March, 2017 - [redacted] ([redacted] performs internal QA and extent of condition on CIP-007 requirements and identifies the omissions.
Mid-April - Response to RFI confirms previously identified omissions.
April 27, 2017 - [redacted] notified of the Potential Violation.
May 17, 2017 - An [redacted] ([redacted] was conducted.
May 25, 2017 - Vulnerability assessment is performed on all asset types within the production environment, including all assets added from July 2016 to March 2017.

What is the violation?

Assets added to a [redacted] production environment have not been actively scanned for vulnerability since 7/1/2016. This violates CIP-010 R3 P3.3 for applicable [redacted] BES cyber system.

Relevant information regarding the identification of the violation(s):

Violation was discovered during an internal QA review performed early March 2017 and was confirmed while collecting data for [redacted] RFI.

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

Milestone 1: This milestone is to perform an extent of condition on all assets in [redacted] ESPs. The intended outcome is to verify new assets that were added into production environment since July 01, 2016. The evidence will show the total number of new assets added since July 01, 2016.

Milestone 2: The intended outcome is to ensure all asset within production environment has went through a vulnerability assessment. The evidence show the vulnerability assessment that was done with action plan to remediate or mitigate vulnerabilities identified in the assessment.

Milestone 3: The intended outcome is to create Standard Work Instruction (SWI) for onboarding assets to guide and educate employee on what need to be done when adding new assets into production. [redacted] will create new NERC CIP assets onboarding SWI. The evidence will show the created SWI.

Milestone4: The intended outcome is to update the [redacted] with the new onboarding process make employee aware that changes have been implemented into the [redacted] process. The evidence will show verification of new assets added to production based on the new onboarding process.

Milestone 5: The intended outcome is communication of newly created SWI and updated [redacted] program and that the updates are enforceable. After completion of Milestone 3 and 4 communication will be sent to SMEs to ensure they are made aware of the changes. The evidence shows an email to SMEs that new SWI is developed, issued, and enforced.

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: November 30, 2017

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Extent of Condition	Verification of all asset added since July 01, 2016 to July 01, 2017.	07/31/2017			No
Vulnerability Assessment	Ensure all new assets added since July 01, 2016 within production environment has went through a vulnerability assessment.	08/30/2017			No
Create new NERC CIP onboarding	Create new NERC CIP assets	10/30/2017			No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
process.	onboarding process to ensure compliance with NERC CIP standards.				
Update [redacted] process.	Update [redacted] process to check verification of new assets added to production based on the new onboarding process.	10/30/2017			No
Communicate newly developed SWI and updated [redacted] process	Communicate changes across business units for milestone 3 and 4.	11/30/2017			No

Additional Relevant Information

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

The Potential Impact to the BES is severe because not performing a vulnerability assessment prior to adding assets into production could introduce security vulnerabilities and impact BES.

The actual impact is minimum because the assets are in an ESP, ports and services are monitored monthly, SIME monitors for successful and failed logons, number of personnel with access is limited, and the firewall rules allow only the required traffic.

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

By completion of the mitigation plan [redacted] will minimize similar issues from occurring. Milestone 1 will verify all new assets were added into production environment since July 01, 2016. Milestone 2 ensure all asset within production environment has went through a vulnerability assessment and action plan to remediate or mitigate vulnerabilities identified in the assessment and vulnerabilities. Milestone 3 [redacted] will create new NERC CIP assets onboarding process to guide and educate employee on what need to be done when adding new assets into production.

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.

2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.

3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

[redacted] Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: [redacted]

Title: [redacted]

Authorized On: [redacted]

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request 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)

Registered Entity Name: [redacted]
NERC Registry ID: [redacted]
NERC Violation ID(s): RFC2017017836
Mitigated Standard Requirement(s): CIP-010-2 R3.
Scheduled Completion as per Accepted Mitigation Plan: November 30, 2017
Date Mitigation Plan completed: November 20, 2017
RF Notified of Completion on Date [redacted]
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017836 Certification Package.zip	File "RFC2017017836 Certification Package.zip" contains coversheet for the package and also the supporting evidence for each milestone.	6,702,560

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

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

Mitigation Plan Verification for RFC2017017836

[redacted]

Standard/Requirement: CIP-010-2 R3

NERC Mitigation Plan ID: RFCMIT013048

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	11/16/17

Description of Issue

In March 2017, during an internal Quality Assurance review it was discovered that [redacted] was routinely not performing an active vulnerability assessment prior to adding assets into the production environment. Assets added into a [redacted] production environment have not been actively scanned for vulnerability since 7/1/2016. This violates CIP010 R3 P3.3 for applicable [redacted] BES cyber system.

The [redacted] ([redacted] process did not include process to assess "new" assets added to production.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017017836 Certification Package	CIP-010-2 R3

Verification of Mitigation Plan Completion

Milestone 1: Extent of Condition.

Proposed Completion Date: July 31, 2017

Actual Completion Date: July 31, 2017

File 1, "*RFC2017017836 Certification Package*", Milestone 1 describes the process used to verify all assets that were added between July 1, 2016, and July 1, 2017.

[redacted] stated the following process:

In order to develop this list, we initially defined a data set of ALL BCS List "changes" for the period July 1, 2016 – July 1, 2017 using our current BCS List as the input, filtering assets that identified asset change in the meta data.

We further defined the data subset [redacted]related assets" from the data set noted above filtering by "[redacted]related asset identifier" meta data. The result was a list of [redacted] assets that were in some way changed during this period.

We then reviewed change records for all [redacted] assets. [redacted] assets were identified using this process as newly added devices and [redacted] identified as replacement adds. The resulting list of [redacted] assets were further evaluated in milestone 2 to determine inclusion in the vulnerability assessment process.

Number of Assets Added:

This sheet shows [redacted] assets were added between July 1, 2016, and July 1, 2017, and [redacted] assets were replaced between July 1, 2016, and July 1, 2017.

Assets in Operation:

This sheet shows the [redacted] assets with a status of "ADD" that are the new assets added between July 1, 2016, and July 1, 2017.

Milestone # 1 Completion verified.

Milestone 2: Vulnerability Assessment.

Proposed Completion Date: August 30, 2017

Actual Completion Date: August 20, 2017

File 1, "*RFC2017017836 Certification Package*", Milestone 2 the [redacted] assets that were added since 7/1/2016 went through a vulnerability assessment.

The document titled "[redacted] CIP010 R3 VULNERABILITY ASSESSMENT CHECKLIST" shows the assets were added since July 01, 2016 to July 01, 2017 within production environment has went through a vulnerability assessment.

Paper assessment was performed on two out of thirteen assets. Those Assets are [redacted] and [redacted] It was not possible to perform an active scan on [redacted]

Below are the [redacted] assets added since July 01, 2016:

[redacted]

[redacted]

Below is the evidence to demonstrate that a vulnerability assessment was performed on the [redacted] new assets. The evidence includes results from vulnerability scans and the discovered vulnerabilities on the [redacted] new assets.

[redacted]

Milestone # 2 Completion verified.

Milestone 3: Create new NERC CIP onboarding process.

Proposed Completion Date: October 30, 2017

Actual Completion Date; October 27, 2017

File 1, "*RFC2017017836 Certification Package*", Milestone 3 the document titled "NERC CIP [redacted] PROCESS" shows the new developed [redacted] Process. The purpose of this process to implement an Access management Process for managing the lifecycle of BES Cyber Systems and their associated BES Assets, PCAs, PACS, and EACMS.

This process describes the high-level steps to:

- Manage the addition, modification, and decommissioning of Assets;
- Execute the change management process during the lifecycle; and
- Produce the specific compliance documentation during the lifecycle.

NERC CIP [redacted]Process, v1, dated January 1, 2018 - This is the Access Management process for managing the lifecycle of BES Cyber Systems and their associated BCAs, PCAs, PACS, and EACMS. Section 4 [redacted]Process (page 3) is a process flow diagram. [redacted]

Milestone # 3 Completion verified.

Milestone 4: Update [redacted] process.

Proposed Completion Date: October 30, 2017

Actual Completion Date: October 27, 2017

Milestone 4 – Submit.pdf

File 1, "*RFC2017017836 Certification Package*", Milestone 4, the document titled [redacted]R-[redacted] shows the updated [redacted] process to check verification of new assets added to production based on the new NERC CIP [redacted] Process (onboarding process).

[redacted] ver 3.4 dated January 1, 2018 - This process supports consistent and correct management of configuration changes to Bulk Electric System (BES) Cyber Assets (BCAs). Section 3 Scope (page 2) shows that the new [redacted]Process is a

prerequisite to this process. [redacted] to add the reference for the new [redacted] Process.

Milestone # 4 Completion verified.

Milestone 5: Communicate newly developed SWI and updated [redacted] process.

Proposed Completion Date: November 30, 2017

Actual Completion Date: November 16, 2017

File 1, "*RFC2017017836 Certification Package*", Milestone # 5 the document titled "New process document – NERC CIP [redacted] PROCESS" shows an email communication to SMEs to inform them of the new developed document "NERC CIP [redacted] PROCESS" and updating the [redacted] ([redacted] process to reflect the addition of the document.

Email Communication - Email from [redacted] on November 16, 2017, stating there is a new NERC CIP [redacted] Process going into effect on January 1, 2018.

[redacted] update - Email from [redacted] on November 16, 2017, stating the [redacted] Process was changed to list the NERC CIP [redacted] PROCESS as a prerequisite.

Milestone # 5 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: [redacted]

Anthony Jablonski
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-010-2
Requirement: CIP-010-2 R3.
Date Submitted: October 17, 2017
Has this violation previously been reported or discovered?: No

Entity Information:

Joint Registration Organization (JRO) ID:
Coordinated Functional Registration (CFR) ID:
Contact Name: [redacted]
Contact Phone: [redacted]
Contact Email: [redacted]

Violation:

Violation Start Date: March 29, 2017
End/Expected End Date:
Reliability Functions: [redacted]
Is Possible Violation still occurring?: No
Number of Instances: 1
Has this Possible Violation been reported to other Regions?: No
Which Regions:
Date Reported to Regions:
Detailed Description and Cause of Possible Violation: *Detailed Description:

Background
The [redacted] installations began at [redacted] in Jan 2017. [redacted] NERC ESP's were in scope for [redacted] installation:
1. [redacted]
2. [redacted]

Incident description
On 9/6/17 [redacted] learned that the [redacted] equipment was plugged into the production environment at [redacted] without performing a vulnerability assessment. During the [redacted] performed on 9/22/17 it was determined that, no [redacted] asset had been plugged into the [redacted] ESP. There had been installations performed in the [redacted] and [redacted] network for [redacted] but none within the [redacted] ESP.
Additionally, [redacted] ESP being a [redacted] ESP and not [redacted] the CIP10 R 3 P3.3 did not apply.
However, [redacted] took this opportunity to determine the extent of condition of a similar possibility within ongoing installations of [redacted] assets at [redacted] ESP's and determined that [redacted] and [redacted] assets of [redacted] were added to the production environment of two [redacted] BES Cyber System ([redacted] and [redacted] ESP) without the execution of an active vulnerability assessment prior to

the assets being connected to the ESPs. These assets had been added to the production ESP on 03/29/2017.[redacted];

*What is the problem?
Beginning 03/29/2017, 'New' cyber assets ([redacted] and [redacted] were added to the production environment of a [redacted] BES Cyber System without an active vulnerability assessment. The [redacted] assets were neither replacements nor part of a CIP exceptional circumstances.
This has been recorded as a violation of CIP-010- R3 P3.3 - "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 and existing baseline configuration of the previous or other existing Cyber Asset".

*Root Cause of Possible Violation:
As per the RCA performed on 10/12/17, the root cause was identified to be the lack of an [redacted] process for NERC CIP assets, that provides a stepwise guide to trigger the proper change management requests and subsequently ensure the collect and verification of evidence during lifecycle of assets throughout installation, maintenance and retirement of assets. [redacted] utilizes a robust Change Management process that is focused on the individual changes that impact asset baselines. The RCA identified that a defined [redacted] process is required to ensure the proper change orders, and correlated evidence, is initiated during each step of the lifecycle of installation of new assets from the point of taking physical possession, the asset is powered and connected to the network, software is installed and configured, and ultimately the asset is placed in production for operational use.

*How was the violation discovered?
Post go-live of a new asset, [redacted] uses the [redacted] for monitoring compliance of all production assets. Output of the [redacted] is reviewed by [redacted] monthly.

On 9/6/17 an [redacted] employee involved with validating compliance to NERC CIP standards and hence collecting testing evidence for [redacted] implementations, reported a possibility that [redacted] equipment was plugged into the 'production environment' without performing a vulnerability assessment. [redacted] investigated the possible violation and extent of condition to conclude the reported CIP 10 R3 P3.3 violation.

*Explain how is it determined that the Noncompliance is related to documentation, performance, or both.

On examining the root cause listed above, it was determined that the noncompliance is related to lack of a documented [redacted] This includes, but is not limited to, triggering the required change orders at the appropriate asset life cycle step and collection of evidence when a NERC CIP asset is first identified and scoped to be a BES Cyber Asset following through to when the asset is plugged into a production ESP and identified as operational to support the BES.

*Timeline:
Beginning 3/18/17 : New cyber assets for [redacted] were activated in [redacted] ESP's within [redacted] ([redacted] and [redacted] ESP)
9/6/17 : [redacted] learnt of a possible violation related to failure to perform [redacted] when [redacted] assets were added to the production environment.
9/22/17 : [redacted] performed an [redacted] and determined that per the project implementation schedule for [redacted] no new cyber assets had been placed in the [redacted] ESP as of the date of [redacted]
10/12/17 : [redacted] performed an extent of condition to confirm that [redacted] equipment ([redacted] was activated in [redacted] ESP's

without an active vulnerability scan.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Corrective Activities:
[redacted] scanned the assets post production and is in process of developing the remediation plan for the vulnerabilities identified.

Mitigating Activities:
Define and communicate An [redacted] program for NERC CIP assets : [redacted] is working to define an [redacted] to trigger the current Change Management process throughout the stages of a NERC CIP asset's lifecycle. This program will be developed and communicated to all authorized NERC CIP users by October 31, 2017. Additionally, [redacted] will re-emphasize the use of a CIP 10 R3 R3.4 based template by the [redacted] to ensure that all medium to high severity vulnerabilities that are scanned via the [redacted] scan, have a recorded action item with an assigned ownership and closing date to address the vulnerability. This will be re-emphasized through the [redacted]

Preventative Measures:
To prevent such occurrences in the future, the [redacted] program would be integrated with the weekly NERC CIP [redacted] meetings to monitor key compliance milestones.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe

Actual Impact to BPS: Moderate

Description of Potential and Actual Impact to BPS:

Actual Impact
New cyber assets for [redacted] were introduced to [redacted] ESP without an active vulnerability scan. This included [redacted] and [redacted] The [redacted] equipment of [redacted] by virtue of hardware design, does not allow for vulnerability scan assessments and this fact is known to all [redacted] clients within the industry and controlled via the [redacted] Terms and Conditions. [redacted]
The [redacted] assets were activated in the [redacted] ESP's beginning 03/29/2017 and the first vulnerability scan was performed on 05/18/2017, following the activation. There was a gap of five weeks before a vulnerability review was performed after the assets were activated within the [redacted] ESP's.
The [redacted] scan has since been performed periodically (first detected 03/18/2017 to last detected 10/03/2017) for [redacted] assets deployed within the [redacted] network. There is more rigor to review [redacted] severity vulnerabilities since September 2017.
[redacted] assessed the actual risk at Medium.

Potential Impact
Potential impact of installing a new cyber asset without a scan could have been severe, since the first scan happened 5 weeks post the equipment was plugged into the production ESP.
However, a [redacted] scan in May 2017 did not reveal severe level vulnerabilities. The scans were more medium severity for the [redacted] equipment , ranging at a level 3 on a scale of 5. There has been a review of high level vulnerabilities to contain risk since May, with the reviews gaining more rigour in September 2017 once the new project team was [redacted] has

been functional and re-organized.

Risk Assessment of Impact to BPS: Since a [redacted] scan was performed at a weekly interval post the installation of the [redacted] assets on the production ESP's, the impact of the [redacted] installation without an active vulnerability scan posed a medium risk to BES.

There is currently a rigor maintained through the [redacted] to evaluate the severity and resulting actions from the vulnerability scans.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
RFC2017018498	CIP-010-2 R3.	

Mitigation Plan Submitted On: January 03, 2018

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: January 17, 2018

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

(1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
(2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
(3) The cause of the Alleged or Confirmed Violation(s).
(4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
(5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
(6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
(7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
(8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
(9) Any other information deemed necessary or appropriate.
(10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
(11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

• The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.

• This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.

• If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.

• Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.

• Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.

• The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [redacted]

NERC Compliance Registry ID: [redacted]

Address: [redacted]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [redacted]

Title: [redacted]

Email: [redacted]

Phone: [redacted]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017018498	03/29/2017	CIP-010-2 R3.
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 R3– Vulnerability Assessments.		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

Brief Description: (What happened?)

Background
The [redacted] installations began at [redacted] in Jan 2017. [redacted] NERC ESP's were in scope for [redacted] installation:
1. [redacted]
2. [redacted]

Incident description
On 09/06/17 [redacted] ([redacted] learned that the [redacted] equipment was plugged into the production environment at [redacted] without performing a vulnerability assessment. During the [redacted] performed on 9/22/17 it was determined that, no [redacted] asset had been plugged into the [redacted] ESP. There had been installations performed in the [redacted] and [redacted] network for [redacted] but none within the [redacted] ESP. Additionally, [redacted] ESP being a [redacted] ESP and not [redacted] the CIP10 R 3 P3.3 did not apply. However, [redacted] took this opportunity to determine the extent of condition of a similar possibility within ongoing installations of [redacted] assets at [redacted] ESP's and determined that [redacted] and [redacted] assets of [redacted] were added to the production environment of two [redacted] BES Cyber System ([redacted] and [redacted] ESP) without the execution of an active vulnerability assessment prior to the assets being connected to the ESPs. These assets had been added to the production ESP on 03/29/2017.

Updated Mitigation Plan on 12/7/2017
[redacted] met with business SME to review and validate if ALL applicable CIP requirements for [redacted] deployment. It was learnt that the evidence for the CIP 007 R5 and CIP009 R1 requirements was not available. Attached file "ComplianceMatrix_[redacted]pdf" shows [redacted] review of all CIP requirements as performed with business SME's.

Cause: (what caused the violation?)
Violation of CIP-010- R3 P3.3 was caused when assets were connected to the production ESP without a vulnerability assessment.

Results of the RCA: (What is the root cause?)
As per the RCA performed on 10/12/17, the root cause was identified to be the lack of an [redacted] process for NERC CIP assets, that provides a stepwise guide to trigger the proper change management requests and subsequently ensure the collect and verification of evidence during lifecycle of assets throughout installation, maintenance and retirement of assets. [redacted] utilizes a robust Change Management process that is focused on the individual changes that impact asset baselines. The RCA identified that a defined [redacted] process is required to ensure the proper change orders, and correlated evidence, is initiated during each step of the lifecycle of installation of new assets from the point of taking physical possession, the asset is powered and connected to the network, software is installed and configured, and ultimately the asset is placed in production for operational use.

Relevant information regarding the identification of the violation(s):

Post go-live of a new asset, [redacted] uses the [redacted] for monitoring compliance of all production assets. [redacted] of the [redacted] is reviewed by [redacted] monthly.

On 09/06/17 an [redacted] employee involved with validating compliance to NERC CIP standards and hence collecting testing evidence for [redacted] implementations, reported a possibility that [redacted] equipment was plugged into the 'production environment' without performing a vulnerability assessment. [redacted] investigated the possible violation and extent of condition to conclude the reported CIP 10 R3 P3.3 violation.

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

Milestone 1- Create an [redacted] program for NERC CIP assets
[redacted] is working to create an [redacted] to trigger [redacted] current Change Management process throughout the stages of a NERC CIP asset's lifecycle.

Purpose of the [redacted] is to help SMEs to be compliant throughout the lifecycle of the asset from commissioning to retirement. The program includes determination of asset's NERC CIP classification (BCA, PCA, EACMS, etc..), use of correct change order type, adding the asset to CIP002 database, and perform vulnerability scanning during staging (pre-production).
[redacted] ([redacted] reviews the evidence of compliance throughout the lifecycle.
This milestone was completed on October 29, 2017.

Milestone 2- Communicate an [redacted] program for NERC CIP assets
Communicate the [redacted] program to all authorized NERC CIP users. This milestone was completed on November 16, 2017.

Milestone 3 - Scan the installed [redacted] assets for vulnerabilities and develop remediation plan
[redacted] scanned the assets post production and is in process of developing the remediation plan for the vulnerabilities identified. Four (4) of the five (5) high priority vulnerabilities from the September scan were mitigated as of Oct 17,2017 for all [redacted] equipment.

An action plan to track the vulnerabilities identified in scan will be recorded in [redacted] CIP010 R3.4 template and will be tracked to completion using [redacted]

Milestone 4 - Validate all CIP requirements for [redacted] Assets
Validate and bring [redacted] assets to compliance for the following requirement by 12/25/2017:
1. CIP-007-6 R5 : Complete [redacted] NERC-CIP System Access Control Procedures Template
2. CIP-009-6 R1 : Create CIP -009 System Recovery Plan

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: January 17, 2018

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Create an [redacted] e program for NERC CIP assets	[redacted] will create an [redacted] program to trigger the current Change Management process throughout the stages of a NERC CIP asset's	[redacted]	10/29/2017		No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
	lifecycle.				
Communicate an [redacted] program for NERC CIP assets	Communicate the defined [redacted] program to trigger the current Change Management process throughout the stages of a NERC CIP asset's lifecycle.	11/16/2017	11/16/2017		No
Scan the installed [redacted] assets for vulnerabilities and develop remediation plan	[redacted] scanned the assets post production and a remediation plan is created to mitigate the vulnerabilities identified.	12/11/2017			No
Bring [redacted] back to compliance with CIP007 R5 and CIP009 R1	SME will generate evidence of compliance for CIP007 R5 and CIP009 R1 as per [redacted] templates.	01/17/2018			No

Additional Relevant Information

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

Identification of Risk : [redacted] has not identified any risk to the BES. Even though there was a gap of five weeks before a vulnerability review was performed after the assets were activated within the [redacted] ESP's, the [redacted] scan has since been performed periodically (first detected 03/18/2017 to last detected 10/19/2017) for [redacted] assets and there is a team to review and remediate vulnerabilities.
Since a [redacted] scan is performed at a weekly interval post the installation of the [redacted] assets on the production ESP's, the impact of the [redacted] installation without an active vulnerability scan posed a medium risk to BES. There is currently a rigor maintained through the [redacted] to evaluate the severity and resulting actions from the vulnerability scans.

Assessment of Potential Impact :
Potential impact of installing a new cyber asset without a scan could have been severe, since the first scan happened 5 weeks post the equipment was plugged into the production ESP.
However, a [redacted] scan in May 2017 did not reveal severe level vulnerabilities. 4 of the 5 vulnerabilities from the September 2017 [redacted] scan that were medium to high level priority, were already corrected by Oct 17, 2017.
There has been a consistent review of high level vulnerabilities to contain risk since May, with the reviews gaining more rigour in September 2017 once the new project team was [redacted] has been functional and re-organized.

Action proposed : These include remediating vulnerabilities for all [redacted] equipment and maintaining check through [redacted] in addition to setting up an [redacted] Program, which triggers the appropriate level of action at different stages of a lifecycle through the [redacted] team.

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

In order to address future BES reliability risk [redacted] has taken several steps to both address the violation identified in this mitigation plan and to prevent possible reoccurrences of this violation. Since [redacted] has now been developed and communicated, any asset introduced , managed and retired from service will have a set of requirements that would need to be met for documentation, evidence and procedure. This would be a long term solution and will assist all assets.

Additionally, for [redacted] in particular, the remediation efforts are to scan vulnerabilities for all equipment and resolve the same.

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.

2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.

3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

[redacted] Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: [redacted]

Title: [redacted]

Authorized On: November 17, 2017

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request 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)

Registered Entity Name: [redacted]
NERC Registry ID: [redacted]
NERC Violation ID(s): RFC2017018498
Mitigated Standard Requirement(s): CIP-010-2 R3.
Scheduled Completion as per Accepted Mitigation Plan: January 17, 2018
Date Mitigation Plan completed: January 17, 2018
RF Notified of Completion on Date: January 18, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017018498 Certification Package.zip	File RFC2017018498 Certification Package.Zip contains cover page for whole package and also evidence supporting each milestone.	3,827,981

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Mitigation Plan Verification for RFC2017018498

[redacted] ([redacted])

Standard/Requirement: CIP-010-2 R3

NERC Mitigation Plan ID: RFCMIT013394-1

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 10/17/17	01/03/18	01/04/18	01/26/18	01/18/18	01/17/18

Description of Issue

Mitigation Task RFC2017018498

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017018498 Certification Package	CIP-010-2 R3
File 2	RFC2017018498 Milestone 4 Submit	CIP-010-2 R3

Verification of Mitigation Plan Completion

Milestone 1: Create an [redacted] program for NERC CIP assets.

Proposed Completion Date: October 31, 2017

Actual Completion Date: October 27, 2017

File 1, "*RFC2017018498 Certification Package*", Milestone 1- Submit, Pages 1 through 13, shows the first revision of the entity define [redacted] process.

Milestone # 1 Completion verified.

Milestone 2: Communicate an [redacted] program for NERC CIP assets.

Proposed Completion Date: November 16, 2017

Actual Completion Date: November 30, 2017

File 1, "*RFC2017018498 Certification Package*", Milestone 2 – Submit, Pages 1 through 3, show the distribution to the entity CIP SMEs on 11-30-2017 also stating that the process will become active Jan 1, 2018.

Milestone # 2 Completion verified.

Milestone 3: Scan the installed [redacted] assets for vulnerabilities and develop remediation plan.

Proposed Completion Date: December 11, 2017

Actual Completion Date: November 29, 2017

File 1, "*RFC2017018498 Certification Package*", Milestone 3- Submit, Pages 2 through 4, show the vulnerability assessment results and remediation's taken on behalf of the entity.

Milestone # 3 Completion verified.

Milestone 4: Bring [redacted] back to compliance with CIP007 R5 and CIP009 R1.

Proposed Completion Date: January 17, 2018

Actual Completion Date: January 17, 2018

File 1, "*RFC2017018498 Certification Package*", Milestone 4-Submit, Pages 2 and 3, show a diagram illustrating the two types of intermediate devices in which the entity utilizes. Additionally Pages 4 through 79, show firewall access permissions in which the entity highlighted (in blue) the address non-interactive traffic such as server-to-server applications whilst (yellow) allow interactive access protocols.

Milestone # 4 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: August 22, 2018

Anthony Jablonski
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-010-2

Requirement: CIP-010-2 R3.

Date Submitted: January 10, 2018

Has this violation previously been reported or discovered?: No

Entity Information:

Joint Registration Organization (JRO) ID:

Coordinated Functional Registration (CFR) ID:

Contact Name: [redacted]

Contact Phone: [redacted]

Contact Email: [redacted]

Violation:

Violation Start Date: May 25, 2017

End/Expected End Date: January 31, 2018

Reliability Functions: [redacted]

Is Possible Violation still occurring?: No

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: Current Practice:

[redacted] has established a vulnerability management program to support the CIP010 R3.1 requirement "At least once every 15 calendar months, conduct a paper or active vulnerability assessment." In an effort to comply with the CIP standards, the [redacted] team performed an active vulnerability assessment in the [redacted] test environment and was under the impression that this test would fulfill both the CIP010 R3.1 and R3.2 requirements at the same time.

Incident Description:

On May 25th, 2017 as part of a scheduled [redacted] activity to comply with the CIP010 R3.1 standard all Testing Assets [redacted] were scanned with the [redacted] appliance, which is our current tool for conducting an active vulnerability assessment. As [redacted] is our test environment and has a representative sample of [redacted] assets. Using the [redacted] appliance to scan certain [redacted] assets has been known to cause operational issues in the [redacted] environment. While reading the CIP 010 R3.2 requirement the SME's were under the impression that this test was a more comprehensive and went above and beyond the therefore by complying with R3.2 that compliance with R3.1 was also gained as [redacted] models the baseline configuration of the BES Cyber System [redacted] environment. These decisions were made in an attempt to

provide improved security and to minimize risk to the BES system.

*What is the problem?

The [redacted] team did not complete a paper assessment or an active vulnerability assessment on [redacted] assets within the 15 calendar month constraints of the standard resulting into a violation of CIP010 R3.1.

*Root Cause of Possible Violation:

The root cause of the possible violation is a misunderstanding by the [redacted] team between the CIP010 R3.1 and CIP010 R3.2 standards. In an effort to go above and beyond the standard from a security perspective the [redacted] teams was under the impression that by completing the requirements for CIP010 R3.2 the team would have covered both standards.

*How was the violation discovered?

The violation was discovered by the [redacted] group when examining the evidence for a different self report [redacted] and came to the realization that the CIP-010 R3.1 requirement had not been met nor addressed by the [redacted] team.

*Explain how is it determined that the Noncompliance is related to documentation, performance, or both.

The noncompliance is related to documentation, since the [redacted] team did not understand the scope of what is expected in the post documentation for this test. Also, due to the infrequency of this criteria and only having to perform this test once every 15 months, and the [redacted] teams first encounter with this test, and some confusion on the team's part about what is expected to be provided as evidence, helped to contribute to this potential noncompliance.

*Timeline:
On May 25th, 2017, a [redacted] scan was used to start the assessment for CIP010 R3.2 for a vulnerability scan, which was completed on June 7, 2017 on all [redacted] assets.
In June, 2017 an [redacted] review of the evidence was completed, and no issues were found by the [redacted] office with the evidence provided. The [redacted] review consisted on verification of the data supporting the [redacted] assets only. The scope of the assessment was not assessed.
In November 2017, during the review of the evidence provide for another Self Report, it was determined that the [redacted] team had not done a full vulnerability assessment on all cyber security assets found in the PSP. During this second review of the evidence, it was determined that the CIP010 R3.2 requirement had not fulfilled, so a self report was generated.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

*Description of Mitigating Activities and Preventive Measures:

Immediate Correcting Activities: The immediate corrective activity is to conduct a vulnerability assessment on all [redacted] and [redacted] assets. This will be complete by January 31, 2018. The [redacted] team has decided to use a combination of active and paper assessments based upon risks to the BES. Some of these issues include: 1. The team is worried about taking down the Bulk Electric System, since most of these [redacted] assets are end of life. 2. We are also in the process of doing a complete system upgrade at [redacted] 3. Scanning some of these assets in the past has led to some stability issues with these assets, and affecting the ability of [redacted] to provide power to the BES.

Mitigating Activities:

Self Report

Document the results of the assessment conducted and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.

Preventative Measures:

The preventative measure is to update the program document by providing guidance on when and how to conduct a vulnerability assessment.

Date Mitigating Activities Completed: January 31, 2018

Impact and Risk Assessment:

Potential Impact to BPS: Minimal

Actual Impact to BPS: Moderate

Description of Potential and Actual Impact to BPS: The potential impact to the BES is moderate, as [redacted] has implemented a documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not performed a vulnerability assessment more than 18, months, but less than 21 months, since the last assessment on one of its applicable BES Cyber Systems.

The actual impact to the BES is low, since [redacted] implements multiple security controls some of which are monthly patching, firewalls in place, jump box to authenticate administrative users just to name a few. These controls minimize attack vectors for any vulnerabilities that are found in the [redacted] environment.

Risk Assessment of Impact to BPS: The potential impact to the BPS is Moderate, as [redacted] has implemented a documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not performed a vulnerability assessment more than 18, months, but less than 21 months, since the last assessment on one of its applicable BES Cyber Systems.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2018019048	CIP-010-2 R3.	

Mitigation Plan Submitted On: January 29, 2018

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: April 30, 2018

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

(1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
(2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
(3) The cause of the Alleged or Confirmed Violation(s).
(4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
(5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
(6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
(7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
(8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
(9) Any other information deemed necessary or appropriate.
(10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
(11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

• The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.

• This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.

• If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.

• Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.

• Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.

• The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [redacted]

NERC Compliance Registry ID: [redacted]

Address: [redacted]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [redacted]

Title: [redacted]

Email: [redacted]

Phone: [redacted]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2018019048	05/25/2017	CIP-010-2 R3.
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 R3– Vulnerability Assessments.		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

Brief Description: (What happened?)

Current Practice:
[redacted] has established a vulnerability management program to support the CIP010 R3.1 requirement "At least once every 15 calendar months, conduct a paper or active vulnerability assessment." In an effort to comply with the CIP standards, the [redacted] ([redacted] team performed an active vulnerability assessment in the [redacted] test environment and was under the impression that this test would fulfill both the CIP010 R3.1 and R3.2 requirements at the same time.

Incident Description:
On May 25th, 2017 as part of a scheduled [redacted] activity to comply with the CIP010 R3.1 standard all [redacted] were scanned with the [redacted] appliance, which is our current tool for conducting an active vulnerability assessment, as [redacted] is our test environment and has a representative sample of [redacted] assets. Using the [redacted] appliance to scan certain [redacted] assets has been known to cause operational issues in the [redacted] environment. At the time, it was presumed by the [redacted] SMEs that by complying with R3.2, compliance with R3.1 was implied and since the [redacted] assets model the baseline configuration of the [redacted] assets, the testing performed for R3.2 was more valuable in assessing the vulnerability of the assets, thus, improving security and minimizing risk to the BES.

Cause: (what caused the violation?)
The [redacted] team did not complete a paper assessment or an active vulnerability assessment on [redacted] assets within the 15 calendar month constraints of the standard resulting into a violation of CIP010 R3.1.

Results of the [redacted](What is the root cause?)
The root cause of the possible violation is a misunderstanding by the [redacted] team between the CIP010 R3.1 and CIP010 R3.2 standards. In an effort to go above and beyond the standard from a security perspective the [redacted] team was under the impression that by completing the requirements for CIP010 R3.2 the team would have covered both standards.

Relevant information regarding the identification of the violation(s):

The violation was discovered by the [redacted] group when examining the evidence for a different self report [redacted] and came to the realization that the CIP-010 R3.1 requirement had not been met nor addressed by the [redacted] team.

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

For Milestone 1: The [redacted] team using a combination of paper and active assessments of [redacted] assets will identify all known vulnerabilities of assets not scanned during the yearly assessment. The [redacted] team will document their findings in [redacted] vulnerability assessment checklist template. The filled-out vulnerability assessment checklist template will be the evidence of completion of this milestone. This will be completed by 02/25/2018. By providing this evidence of completion of CIP-010 R3.1 will be satisfied on all [redacted] assets.

Milestone 2: The program document governing vulnerability assessments will be revised to provide clarification for SME's that CIP-010 R3.1 and R3.2 standards are separate. The program document will be revised to CIP-010 R3.1 and R3.2 standards by 3/23/2018. Evidence will be updated program document.

Milestone 3: Upon issuing the revised document (From milestone above) [redacted] will utilize the required reading program to verify that all SME's of [redacted] ESPs, have read and understood the requirements. The evidence will be an excel sheet output from [redacted] System) the completion of required read by all SMEs. This will be completed by 4/30/2018.

Milestone 4: [redacted] business unit maintains a [redacted] that includes tracking of completion of all the CIP requirements. [redacted] will be updated to include annual (12 months) completion of CIP010 R3 Part 3.1 requirements and every 36 months completion of CIP010 R3 Part 3.2. This will be completed by 4/30/2018. Evidence will be [redacted] tracking excel sheet showing CIP010 P3.1 and P3.2 in schedule.

Milestone 5: Extent of condition.
The purpose of this milestone is to verify this condition (Assets without a paper or active assessment) does not exist for other NERC ESPs. This will be completed by 4/30/2018. Evidence will be an analysis sheet by [redacted] QA analyst showing completion of Paper or Active vulnerability assessment for each asset from [redacted] CIP002 list ([redacted] Database).

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: April 30, 2018

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Milestone 1: Conduct a vulnerability assessment on all [redacted] assets not scanned during the yearly assessment.	The [redacted] team has decided to use a combination of active and paper assessments based upon risks to the BES.	02/28/2018			No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Milestone 2: The preventative measure is to update the program document	In the program document provide clarification for SME's that CIP-010 R3.1 and R3.2 standards are separate.	03/23/2018			No
Milestone 3: SME's read the revised CIP010 R3 program	The SME's will use the required read program to verify reading the revised program documentation	04/30/2018			No
Milestone 4: Update [redacted]	The [redacted] will be updated to include annual (12 months) completion of CIP010 R3 requirements.	04/30/2018			No
Milestone 5: Extent of condition	The purpose of this milestone is to verify this condition does not exist for other NERC assets.	04/30/2018			No

Additional Relevant Information

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

The potential impact to the BES is moderate, as [redacted] has implemented a documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable BES Cyber Systems.

The actual impact to the BES is low, since [redacted] implements multiple security controls some of which are monthly patching, firewalls in place, jump box to authenticate administrative users just to name a few. These controls minimize attack vectors for any vulnerabilities that are found in the [redacted] environment.

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

Successful completion of the Mitigation Plan as laid out in Section D will minimize the probability that [redacted] will incur further violations of the CIP-010 R3 standards, since the SMEs will have a better understanding of what is expected of them and improvements to [redacted] will help with completion of the CIP-010 R3 requirements.

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.

2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.

3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

[redacted] Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: [redacted]

Title: [redacted]

Authorized On: January 29, 2018

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request 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)

Registered Entity Name: [redacted]
NERC Registry ID: [redacted]
NERC Violation ID(s): RFC2018019048
Mitigated Standard Requirement(s): CIP-010-2 R3.
Scheduled Completion as per Accepted Mitigation Plan: April 30, 2018
Date Mitigation Plan completed: April 30, 2018
RF Notified of Completion on Date: April 30, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Milestone 1 - Submit.pdf	Due to size limit of files [redacted] has added file name milestone1.pdf as a separate pdf file from the rest of the package in zip file named RFC2018019048.zip	49,312,395
Entity	RFC2018019048 Certification Package.zip	Due to size limit of files [redacted] has added file name milestone1.pdf as a separate pdf file from the rest of the package in zip file named RFC2018019048.zip	25,732,210

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

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

Mitigation Plan Verification for RFC2018019048

[redacted] ([redacted])

Standard/Requirement: CIP-010-2 R3

NERC Mitigation Plan ID: RFCMIT013546

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 01/10/18	01/29/18	02/23/18	03/21/18	04/30/18	05/01/18

Description of Issue

Mitigation Task RFC2018019048

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	Milestone 1- Submit	CIP-010-2 R3
File 2	RFC2018019048 Certification Package	CIP-010-2 R3

Verification of Mitigation Plan Completion

Milestone 1: Conduct a vulnerability assessment on all [redacted] assets not scanned during the yearly assessment.

Proposed Completion Date: February 28, 2018

Actual Completion Date: January 26, 2018

File 1, "*Milestone 1-Submit*", Pages 13 through 5464, show the results of the conducted CVA as required by milestone 1.

Milestone # 1 Completion verified.

Milestone 2: The preventative measure is to update the program document.

Proposed Completion Date: March 23, 2018

Actual Completion Date: March 13, 2018

File 2, "*RFC2018019048 Certification Package*" Milestone 2-Submit, Pages 2 and 15, show the updates as determined by milestone 2. In addition, Pages 52 through 98 show the old/outdated Vulnerability Management Assessment documentation while Pages 2 through 51, show the updated procedure with the incorporated changes previously stated on Pages 2 and 15.

Milestone # 2 Completion verified.

Milestone 3: SME's read to revise CIP010 R3 program.

Proposed Completion Date: April 30, 2018

Actual Completion Date: April 24, 2018

File 3, "*RFC2018019048 Certification Package*"; Milestone 3-Submit, Pages 2 and 3, show that the training was loaded and made available via the entities' [redacted] Application. Page 3, shows the direct output of the individuals who completed the training based on the previous milestones updates.

Milestone # 3 Completion verified.

Milestone 4: Update [redacted]

Proposed Completion Date: April 30, 2018

Actual Completion Date: May 1, 2018

File 3, "*RFC2018019048 Certification Package*", Milestone 4-Submit, Page 3, shows the outdated and old version of the entities' [redacted] worksheet whereas Page 2, illustrates the new [redacted] worksheet created based off of milestone 4 of this mitigation plan. The callout on Page 2 also references the location and requirement of evidence to be collected by this new workbook.

Milestone # 4 Completion verified.

Milestone 5: Extent of condition.

Proposed Completion Date: April 17, 2018

Actual Completion Date: April 17, 2018

File 3, "*RFC2018019048 Certification Package*", Milestone 5-Submit, Page 2 through 287, provide an overview of the assets for which vulnerability assessment scans were missed during the yearly assessments and has now been completed. The Summary section shows that out of the [redacted] assets which were not scanned. Remediation included performing [redacted] active scans and [redacted] paper assessments.

Milestone # 5 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: September 6, 2018

Anthony Jablonski
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Attachment 15

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

15.a The Entity's Self-Report (RFC2017018285);
15.b The Entity's Mitigation Plan designated as RFCMIT013252 submitted [redacted];
15.c The Entity's Certification of Mitigation Plan Completion dated [redacted];
15.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted], 2017;
15.e The Entity's Self-Report (RFC2017018761);
15.f The Entity's Mitigation Plan designated as RFCMIT013445 submitted [redacted];
15.g The Entity's Certification of Mitigation Plan Completion dated [redacted];
15.h ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted]

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-010-2

Requirement: CIP-010-2 R4.

Date Submitted: August 24, 2017

Has this violation previously been reported or discovered?: No

Entity Information:

Joint Registration Organization (JRO) ID:

Coordinated Functional Registration (CFR) ID:

Contact Name: [redacted]

Contact Phone: [redacted]

Contact Email: [redacted]

Violation:

Violation Start Date: May 17, 2017

End/Expected End Date:

Reliability Functions: [redacted]

Is Possible Violation still occurring?: No

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: *Detailed Description:
On or about May 17th, during the monthly patching of the [redacted] assets, the firmware update provided by the vendor changed the password of the [redacted] switch to a previously used password, not the manufacture default. (Note: The password was returned to its current state on May 22nd). The [redacted] representative assigned to the [redacted] team could not log into the switch using the current password after the firmware was updated. A ticket was opened with the vendor [redacted] and their recommendation was to attempt to log into the [redacted] switch directly with a console. The individual engaged in troubleshooting found a laptop in the [redacted] on a "crash cart". He assumed that this was an authorized TCA. He connected the laptop to the asset [redacted] via a serial connection. The attempt to login using the serial connection failed. [redacted] was contacted and asked that the laptop stay connected until the technician arrived onsite. [redacted] sent a technician onsite on May 19th and he was unable to connect to the asset. When the technician had completed his activities, they forgot to disconnect the laptop form the asset. The laptop remained connected until June 20th when it was discovered during a pre-[redacted] The [redacted] team supervisor was contacted and the laptop was disconnected from the asset. The laptop is a [redacted] machine with no network connection and unknown patch and antivirus update history. Since this was unauthorized device used as TCA this was a violation of CIP-010-2 R4.

Self Report

*Root Cause of Possible Violation:
The SME assumed that the laptop in the datacenter was an authorized TCA.

*How was the violation discovered?
This violation was discovered during a pre-[redacted] of the [redacted] The pre-[redacted] team immediately contacted the [redacted] Supervisor. Within minutes, the supervisor entered the [redacted] and removed the serial cable connected to the asset. The time between the discovery of the incident and the reporting of the incident was to allow for the [redacted] Supervisor to investigate the incident and determine who and why the laptop was connected.

*Timeline:
17-May Laptop connected to the asset to conduct troubleshooting
19-May [redacted] technician arrived onsite to help in troubleshooting efforts
20-Jun Pre-[redacted] team discovered the laptop and it was disconnected from the asset.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Mitigating Activities:
The un-validated assumption that this laptop was available for the use within the [redacted] Computer room ([redacted] team is one of many groups with access within this space) is mitigated by labeling the laptop "DO NOT USE FOR NERC CIP".
Preventative Measures:
As the need for a TCA has been identified, the [redacted] team will follow the "Transient Cyber Asset and Removable Media program" to add an authorized TCA for their use.
This issue will also be communicated to all SMEs via a discussion during the next C3 (Knowledge Sharing) session as well as a Program awareness communication via [redacted] email list.
In addition, a target communication with the authorized TCA users (including newly identified [redacted] personnel) describing: 1) this issue, 2) summarizing the TCA requirement, 3) program document location and 4) program SME to contact with any additional questions in the future. All recipients will be required to send an acknowledgment to this email.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: [redacted] is a [redacted] Switch running [redacted] This [redacted] Switch is associated with the [redacted] and as such, is not directly used for the operation of the BCS. This supports the asset is classification as a PCA.

The firmware update changed the login password and neither a remote login nor a physical connection could be made to the asset. As neither the [redacted] representative attached to the [redacted] ([redacted] team nor the [redacted] technician could login to the asset no code could be transferred or setting could be changed from the laptop.

[redacted] has a program that governing the Transient Cyber Asset and Removable Media program. While the [redacted] team does not have a list of authorized TCA user or devices, the [redacted] team does fully comply with the Removable Media requirements. The [redacted] representative attached to the [redacted] ([redacted] team is authorized to use Removable Media on assets in the [redacted]

Self Report

Risk Assessment of Impact to BPS:

The risk to the reliability of the BPS remains minimal. While connecting an uncontrolled laptop directly to an asset introduces a new attack vector into an asset contained in a High ESP, as stated above the asset is classified as a PCA. The risk is low as the laptop was not wirelessly connected to another network.

[redacted] is included in the [redacted] project, that validates that patches are evaluated and applied monthly (to comply with CIP-007 R2.2 and R2.3) and its baseline is monitored for changes (to comply with CIP-010 R2.1). This means that the asset's patches are up-to-date minimizing the software vulnerabilities in the asset. While no one could login to the asset during the troubleshooting, the baseline monitoring would have detected any changes to software if an unidentified vulnerability had exploited via new software being added while the laptop was connected.

In addition, the asset and any logically connected devices are protected by several other methods included in [redacted] defense-in-depth strategy including their malicious code prevention methods and [redacted] monitoring

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017018285	CIP-010-2 R4.	

Mitigation Plan Submitted On: September 21, 2017

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: October 20, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

(1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
(2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
(3) The cause of the Alleged or Confirmed Violation(s).
(4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
(5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
(6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
(7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
(8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
(9) Any other information deemed necessary or appropriate.
(10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
(11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

• The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.

• This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.

• If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.

• Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.

• Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.

• The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [redacted]

NERC Compliance Registry ID: [redacted]

Address: [redacted]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [redacted]

Title: [redacted]

Email: [redacted]

Phone: [redacted]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017018285	05/17/2017	CIP-010-2 R4.
Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, 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.		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

Brief Description: (What happened?)
On or about May 17th, during the monthly patching of the [redacted] assets, the firmware update provided by the vendor changed the password of the [redacted] switch to a previously used password, not the manufacture default. (Note: The password was returned to its current state on May 22nd). The SME, a [redacted] representative assigned to the [redacted] ([redacted] team, could not log into the switch using the current password after the firmware was updated. A ticket was opened with the vendor ([redacted] and their recommendation was to attempt to log into the [redacted] switch directly with a console. The SME engaged in troubleshooting located a laptop in the [redacted] He assumed that this was an authorized TCA. He connected the laptop to the asset ([redacted] via a serial connection. The attempt to login using the serial connection failed. [redacted] was contacted and asked that the laptop stay connected until the technician arrived onsite. [redacted] sent a technician onsite on May 19th and he was unable to connect to the asset. When the SME completed his activities, the laptop was not disconnected from the asset. The laptop remained connected until June 20th, when it was discovered during a pre-[redacted] The [redacted] team supervisor was contacted and the laptop was disconnected from the asset. The laptop is a [redacted] machine with no network connection and unknown patch and antivirus update history. Since this was an unauthorized device used as a TCA this was a violation of CIP-010-2 R4.

Cause: (what caused the violation?)
A laptop was in the datacenter on a cart and it was not an authorized TCA.

Results of the RCA: (What is the root cause?)
The SME assumed that the laptop in the datacenter was an authorized TCA.

Relevant information regarding the identification of the violation(s):

This violation was discovered during a pre-[redacted] of the [redacted] The pre-[redacted] team immediately contacted the [redacted] Supervisor. Within minutes, the supervisor entered the [redacted] and removed the serial cable connected to the asset. The time between the discovery of the incident and the reporting of the incident was to allow for the [redacted] Supervisor to investigate the incident and determine who and why the laptop was connected.

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

ID [redacted] TCA users (Milestone #1)
This milestone is for the supervisor of the [redacted] ([redacted] team to identify and list the individuals in his group that will need access to Transient Cyber Asset (TCA). The supervisor's list of authorized individuals will be entered into the [redacted] ([redacted] The access to the TCA for [redacted] will be handled in the same manner and for the other TCAs, via [redacted] Note: Milestones 1 - 4 are required by the TCA program to authorize a new device for the [redacted] team's use. These four milestones as an aggerate will prevent the root cause by authorizing a TCA for use in the [redacted]

ID TCA requirements (Milestone #2)
This event has identified a need for a TCA by the [redacted] team and they will need to determine the device's requirements. The list of requirements will be the input to Milestone #3.

Determine Technical Solution for TCA (Milestone #3)
From the list of requirements in Milestone #2, the TCA device make and model will be identified and procured. Once the TCA is procured, the "Transient Devices and Removable Media Program" will be followed.

Implement TCA solution (Milestone #4)
Following the "Transient Devices and Removable Media Program" the [redacted] team will add the newly procured TCA into the program. This along with Milestone #1 will give authorized [redacted] personal access to an authorized TCA.

Investigate unauthorized TCA (Milestone #5)
As the laptop that was the only identified device during the initiating [redacted] it will be investigated. If the device is not needed for NERC-CIP equipment it will be labeled so that it will not be plugged into a NERC-CIP asset. If it is needed for NERC-CIP equipment it will be added to the authorized list following the "Transient Devices and Removable Media Program"

Program awareness communication (Milestone #6)
This is one communication method of three Milestones (Milestones 6, 7 & 8) being used to reinforce the TCA / RM program with the SMEs. For this milestone, a communication will be distributed via email to the Subject Matter Experts (SMEs) that work on NERC-CIP assets. This email will provide a summary of the event, the high-level requirements for TCAs and the document links.

Add discussion to C3 session agenda (Milestone #7)
Monthly meetings are held between the [redacted] ([redacted] and the NERC-CIP SMEs. These meetings are to discuss upcoming changes to NERC documentation, bring up issues the SMEs are running into, etc. This Possible Non-Compliance will be added to the agenda so that the issue can be reviewed and the process discussed with the SMEs.

Targeted communication with TCA users (Milestone #8)
A communication will be distributed via email to SMEs that have been granted access to a TCA. This email will reiterate the program at a high level and contain a link to the program document. This communication will require a confirmation email from each SME stating that they are required to review the email and the program document and understand the program.

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: October 20, 2017

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
ID TCA requirements	Create a list of requirements for the [redacted] TCA	07/18/2017	07/18/2017		No
Investigate unauthorized TCA	Determine if the laptop in the [redacted] is needed for NERC-CIP support	07/18/2017	07/18/2017		No
ID [redacted] TCA users	Create a list of [redacted] users that need access to a TCA	07/20/2017	07/20/2017		No
Program awareness communication	Communicate the program to NERC-CIP SMEs	08/02/2017	08/02/2017		No
Determine Technical Solution for TCA	Determine what device meets the requirements of Milestone #2.	08/04/2017	08/04/2017		No
Add discussion to C3 session agenda	Add this PNC to the monthly C3 session	08/31/2017	07/27/2017		No
Implement TCA solution	Implement TCA solution made in Milestone #3	09/29/2017			No
Targeted communication with TCA users	Provide communication with required feedback to NERC-CIP SMEs with access to a TCA	10/20/2017			No

Additional Relevant Information

Milestone 2 ID TCA requirements 7/18/2017
Milestone 5 Investigate unauthorized TCA 7/18/2017
Milestone 1 ID [redacted] TCA users 7/20/2017
Milestone 6 Program awareness communication 8/2/2017
Milestone 3 Determine Technical Solution for TCA 8/4/2017
Milestone 7 Add discussion to C3 session agenda 8/31/2017
Milestone 4 Implement TCA solution 9/29/2017
Milestone 8 Targeted communication with TCA users 10/20/2017

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

[redacted]MNG is a [redacted] Switch running [redacted]. This [redacted] Switch is associated with the [redacted] and as such, is not directly used for the operation of the BES. This supports the asset classification as a PCA.

The firmware update changed the login password and neither a remote login nor a physical connection could be made to the asset. As neither, the [redacted] nor the vendor technician could login to the asset, no code could be transferred or setting could be changed from the laptop.

While connecting an uncontrolled laptop directly to an asset introduces a new attack vector into an asset contained in a High ESP, as stated above the asset is classified as a PCA. The risk is low as the laptop was not wirelessly connected to another network.

[redacted] is included in the [redacted] project, that validates that patches are evaluated and applied monthly (to comply with CIP-007 R2.2 and R2.3) and its baseline is monitored for changes (to comply with CIP-010 R2.1). This means that the asset's patches are up-to-date minimizing the software vulnerabilities in the asset. While no one could login to the asset during the troubleshooting, the baseline monitoring would have detected any changes to software if an unidentified vulnerability had exploited via new software being added while the laptop was connected.
In addition, the asset and any logically connected devices are protected by several other methods included in [redacted] defense-in-depth strategy including their malicious code prevention methods and [redacted] monitoring.

In addition, the supervisor of the [redacted] team discussed the event with his team and made it known not to use any TCA until the new TCA had been processed.

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

The TCA/RM program has been communicated to the SMEs for their refamiliarization of the requirements (Milestones 6, 7 & 8). In addition, the laptop that is in the [redacted] has been labeled so that it will not be used as a TCA (Milestones 5) and the [redacted] team will obtain an authorized TCA (Milestones 1, 2, 3 &4).

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.

2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.

3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

[redacted] Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: [redacted]

Title: [redacted]

Authorized On: September 21, 2017

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request 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)

Registered Entity Name: [redacted]
NERC Registry ID: [redacted]
NERC Violation ID(s): RFC2017018285
Mitigated Standard Requirement(s): CIP-010-2 R4.
Scheduled Completion as per Accepted Mitigation Plan: October 20, 2017
Date Mitigation Plan completed: October 13, 2017
RF Notified of Completion on Date: October 18, 2017
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017018285 Certification Package.zip	Zip file RFC2017018285 Certification Package.zip contains the cover page for the violation RFC2017018285 and one file per milestone as an evidence for the completion of the Mitigation Plan.	2,784,820

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Mitigation Plan Verification for RFC2017018285

[redacted] ([redacted])

Standard/Requirement: CIP-010-2 R4

NERC Mitigation Plan ID: RFCMIT013252

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 08/24/17	09/21/17	10/10/17	10/25/2017	10/18/17	10/13/17

Description of Issue

On or about May 17th, during the monthly patching of the [redacted] assets, the firmware update provided by the vendor changed the password of the [redacted] switch to a previously used password, not the manufacture default. (Note: The password was returned to its current state on May 22nd). The SME, a [redacted] representative assigned to the [redacted] ([redacted] team, could not log into the switch using the current password after the firmware was updated. A ticket was opened with the vendor ([redacted] and their recommendation was to attempt to log into the [redacted] switch directly with a console. The SME engaged in troubleshooting located a laptop in the [redacted] He assumed that this was an authorized TCA. He connected the laptop to the asset ([redacted] via a serial connection. The attempt to login using the serial connection failed. [redacted] was contacted and asked that the laptop stay connected until the technician arrived onsite. [redacted] sent a technician onsite on May 19th and he was unable to connect to the asset. When the SME completed his activities, the laptop was not disconnected from the asset. The laptop remained connected until June 20th, when it was discovered during a pre-[redacted] The [redacted] team supervisor was contacted and the laptop was disconnected from the asset. The laptop is a [redacted] machine with no network connection and unknown patch and antivirus update history. Since this was an unauthorized device used as a TCA this was a violation of CIP-010-2 R4.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017018285 Certification Package	CIP-010-2 R4

Verification of Mitigation Plan Completion

Milestone 1: ID TCA requirements.

Proposed Completion Date: July 18, 2017

Actual Completion Date: July 18, 2017

File 1, "*RFC2017018285 Certification Package*", Milestone 2- Submit, Pages 1 through 6, illustrate the requirements identified by the entity for a [redacted] diagnostic Notebook which will be classified as a TCA. This is also identified in Milestone 4- Submit, Pages 1 through 6.

Milestone # 1 Completion verified.

Milestone 2: Investigate unauthorized TCA.

Proposed Completion Date: July 18, 2017

Actual Completion Date: July 18, 2017

File 1, "*RFC2017018285 Certification Package*", Milestone 5-Submit, Page 1, within the description explains that the asset was not required for support while Page 2, shows an image of that device.

Milestone # 2 Completion verified.

Milestone 3: ID [redacted] TCA users.

Proposed Completion Date: July 20, 2017

Actual Completion Date: September 6, 2017

File 1, "*RFC2017018285 Certification Package*", Milestone 1- Submit Pages 1 through 5, illustrate the updating of the users who need access to the TCA produced by entity supervision.

Milestone # 3 Completion verified

Milestone 4: Program awareness communication.

Proposed Completion Date: August 2, 2017

Actual Completion Date: July 27, 2017

File 1, "*RFC2017018285 Certification Package*", Milestone 7-Submit, Pages 1 through 5, shows the meeting invite that discusses the self-report submitted, and the attendee sheet/ sign-in sheet utilized for this meeting.

Milestone # 4 Completion verified

Milestone 5: Determine Technical Solution for TCA.

Proposed Completion Date: August 4, 2017

Actual Completion Date: July 25, 2017

File 1, "*RFC2017018285 Certification Package*", Milestone 3- Submit, Page 5, identifies a [redacted] as the device of choice per this milestone.

Milestone # 5 Completion verified

Milestone 6: Add discussion to C3 session agenda.

Proposed Completion Date: August 31, 2017

Actual Completion Date: July 27, 2017

File 1, "*RFC2017018285 Certification Package*", Milestone 7-Submit, Page 2, illustrates the addition of the PNC to their C3 session agenda in regards to communicating the PNC/ Self-Report of CIP TCAs.

Milestone # 6 Completion verified

Milestone 7: Implement TCA solution.

Proposed Completion Date: September 29, 2017

Actual Completion Date: March 7, 2017

File 1, "*RFC2017018285 Certification Package*", Milestone 4-Submit, Page 17, shows the users added to this device after implementation as previously stated in milestone 2. In addition Page 5, shows the TCA Management and usage requirements.

Milestone # 7 Completion verified

Milestone 8: Targeted communication with TCA users.

Proposed Completion Date: October 20, 2017

Actual Completion Date: October 13, 2017

File 1, "*RFC2017018285 Certification Package*", Milestone8-Submit, Pages 1 through 68, shows the responses from entity NERC-CIP SMEs with access to a TCA in regards to reading and understanding TCA rules and their responsibilities.

Milestone # 8 Completion verified

The Mitigation Plan is hereby verified complete.

Date: November 28, 2017

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-010-2
Requirement: CIP-010-2 R4.
Date Submitted: December 05, 2017
Has this violation previously been reported or discovered?: No

Entity Information:

Joint Registration Organization (JRO) ID:
Coordinated Functional Registration (CFR) ID:
Contact Name: [redacted]
Contact Phone: [redacted]
Contact Email: [redacted]

Violation:

Violation Start Date: October 20, 2017
End/Expected End Date:
Reliability Functions: [redacted]
Is Possible Violation still occurring?: No
Number of Instances: 1
Has this Possible Violation been reported to other Regions?: No
Which Regions:
Date Reported to Regions:

Detailed Description and Cause of Possible Violation:

Detailed Description:
On October 19, a specialist from the [redacted] received a call from Operations reported that a drop in pressure occurred in a [redacted] differential expansion unit. This meant that a new module had to be installed and the software program added to it.
A module was installed on Oct 20 and the TCA was used to program the module. However, the drop in pressure still existed. So, on October 23 the original module was re-added.
During this time the [redacted] specialist had discussions with a specialist from the [redacted] group. Together they mistakenly concluded that no NERC work/documentation was needed for this action.
The module was programmed using the corporate computer used by the SME, which is also a designated TCA. The SME did not capture the evidence that the TCA had all the controls on. Hence a violation of CIP01 R4.
A [redacted] at [redacted] learned of this occurrence of non-compliance with the TCA process on October 23 and submitted a Potential Violation Notification

What is the problem?
Individuals at [redacted] connected to the NERC-CIP assets with transient devices and not following the "[redacted]" program to collect appropriate evidence of compliance.

Self Report

Root Cause of Possible Violation:
Lack of understanding at [redacted] for working with TCA's. This resulted in the SME's not following the "Using Transient Devices and Removable media" procedure.
In this instance the [redacted] (The SME who used the TCA) was not trained on TCA program or program specifics.

How was the violation discovered?
On 10/23/2017 The SME at [redacted] PP learned of the use of TCAs by the [redacted] That SME then concluded that some individuals at [redacted] are connecting to NERC-CIP assets with transient devices and not following the "[redacted]" document.

Explain how is it determined that the Noncompliance is related to documentation, performance, or both.

Not all the site SME's received/acknowledged newly developed TCA program

Timeline:
Call from Operations October 19, 2017
Call from Operations that an [redacted] differential expansion drop in pressure occurred. A new module had to be added

New Module installed October 20, 2017
A new module had to be added and the software program downloaded to it.

Original Reinstalled October 23, 2017
The issue still existed so the original module was re-added.

Discussion with [redacted] October 19, 20 and 23, 2017
Discussions were held with an [redacted] ([redacted] specialist and they concluded that no NERC work/documentation was needed in this instance.

Oct 23, 2017
A Controls Engineer became aware that "[redacted]" procedure was not being followed by the [redacted] and submitted a Potential Violation Notification

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Immediate Correcting Activities:
Current practice was modified to inform [redacted] ([redacted] group members and NOT to touch any of the assets until further notice.

The SME then prepared a retroactive Change Order to explain the work performed, update documentation, and in addition follow the CIP-011 Cyber Asset Reuse and Disposal program

Immediately the [redacted] "[redacted] programs were distributed to the leaders of each group.

The SME from [redacted] who connected the TCA has supplied the label evidence that the laptop that was used was a corporate TCA and would have had anti-virus and patching controls up to date.

Mitigating Activities:
Immediate containment action involved submitting a change order to run a new baseline to verify that the new module did not make any adverse changes. This process included the creation of a test rack that was used to install the new module by resetting it back to the original factory settings

Self Report

Preventative Measures:
Realizing that there was a general lack of understanding of the TCA process, a training session for SME's, including all the groups in [redacted] about the TCA process was conducted on 11/7/2017.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS:
Potential Impact
The potential impact of not following the Transient access procedures include:
•Unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
•Unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Actual Impact:
A new baseline confirmed that there was no adverse impact to the BES.

Risk Assessment of Impact to BPS: A new baseline that was run verified that the new module did not make any changes, thus there was no adverse impact to the BES

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017018761	CIP-010-2 R4.	

Mitigation Plan Submitted On: December 14, 2017

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: December 22, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

(1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
(2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
(3) The cause of the Alleged or Confirmed Violation(s).
(4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
(5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
(6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
(7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
(8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
(9) Any other information deemed necessary or appropriate.
(10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
(11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

• The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.

• This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.

• If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.

• Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.

• Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.

• The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [redacted]

NERC Compliance Registry ID: [redacted]

Address: [redacted]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [redacted]

Title: [redacted]

Email: [redacted]

Phone: [redacted]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017018761	10/20/2017	CIP-010-2 R4.
Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, 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.		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

Current Process
[redacted] follows an established, documented Transient Asset process for updates to NERC assets. Transient Cyber Asset (TCA) and Removable Media (RM) Program requires use of authorized, pre-designated TCA assets by authorized SMEs. The program also requires a minimum set of controls that are required for TCA and gathering of evidence that the controls were in place when the TCA was used.

Incident description
On October 19, a specialist from the [redacted] ([redacted] received a call from Operations reported that a drop in pressure occurred in a [redacted] differential expansion unit. This meant that a new module had to be installed and the software program added to it.

A module was installed on Oct 20 and the TCA was used to program the module. However, the drop in pressure still existed. So, on October 23 the original module was re-added.

During this time the [redacted] specialist had discussions with a specialist from the [redacted] ([redacted] group. Together they mistakenly concluded that no NERC work/documentation was needed for this action.

The module was programmed using the corporate computer used by the SME, which is also a designated TCA. The SME did not capture the evidence that the TCA had all the controls on. Hence a violation of CIP010 R4.

A [redacted] at [redacted] learned of this occurrence of non-compliance with the TCA process on October 23 and submitted a Potential Violation Notification

What is the problem?
Individuals at [redacted] connected to the NERC-CIP assets with transient devices and not following the "[redacted]" program to collect appropriate evidence of compliance.

Root Cause of Possible Violation:
Lack of understanding at [redacted] for working with TCA's. This resulted in the SME's not following the [redacted]" procedure.

Relevant information regarding the identification of the violation(s):

On 10/23/2017 An SME became aware that "[redacted]" procedure was not being followed by the [redacted] and submitted a Potential Violation Notification

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

The following mitigation plans have been planned to address the violation reported in SR#66:
Milestone 1 - Conduct training for all the [redacted] SME's about the TCA process
To address the general lack of understanding of the TCA process, a training session for SME's, including all the groups in [redacted] about the TCA process was conducted on 11/3/2017

Milestone 2 - Prepare a change order and run a new baseline to contain the violation
The SME prepared a retroactive Change Order to explain the work performed. Immediate containment action involved submitting this change order and to run a new baseline to verify that the new module did not make any adverse changes. This process included the creation of a test rack that was used to install the new module by resetting it back to the original factory settings

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: December 22, 2017

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
1. Conduct training for all the [redacted] SME's about the TCA process	To address the general lack of understanding of the TCA process, a training session for SME's, including all the groups in [redacted] about the TCA process was conducted on 11/3/2017	11/03/2017	11/03/2017		No
2. Prepare a change order and run a new baseline to contain the violation	The SME prepared a retroactive Change Order to explain the work performed, update documentation. Immediate containment action involved submitting this change order and to run a new baseline to verify that the new module did	12/22/2017			No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
	not make any adverse changes. This process included the creation of a test rack that was used to install the new module by resetting it back to the original factory settings				

Additional Relevant Information

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

Actual impact was minimal as the transient device had been updated for virus software. In addition, the required training on the TCA program was provided immediately. [redacted] do not foresee risk to the Bulk Electric System (BES).

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

Provide overview surrounding all Transient Device Program Documents and templates -11/3 completed

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.

2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.

3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

[redacted] Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: [redacted]

Title: [redacted]

Authorized On: December 14, 2017

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request 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)

Registered Entity Name: [redacted]
NERC Registry ID: [redacted]
NERC Violation ID(s): RFC2017018761
Mitigated Standard Requirement(s): CIP-010-2 R4.
Scheduled Completion as per Accepted Mitigation Plan: December 22, 2017
Date Mitigation Plan completed: December 21, 2017
RF Notified of Completion on Date: January 17, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017018761 Certification Package.zip	Zip file "RFC2017018761 Certification Package" contains the cover page for the package and also the evidence supporting each milestone.	976,754

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

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

Mitigation Plan Verification for RFC2017018761

[redacted] ([redacted])

Standard/Requirement: CIP-010-2 R4

NERC Mitigation Plan ID: RFCMIT013445

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 12/05/17	12/14/17	01/10/18	02/02/18	01/17/18	02/06/18

Description of Issue

[redacted] follows an established, documented Transient Asset process for updates to NERC assets. Transient Cyber Asset (TCA) and Removable Media (RM) Program requires use of authorized, pre-designated TCA assets by authorized SMEs. The program also requires a minimum set of controls that are required for TCA and gathering of evidence that the controls were in place when the TCA was used. On October 19, a specialist from the [redacted] ([redacted]) received a call from Operations reported that a drop in pressure occurred in a [redacted] differential expansion unit. This meant that a new module had to be installed and the software program added to it.

A module was installed on Oct 20 and the TCA was used to program the module. However, the drop in pressure still existed. So, on October 23 the original module was re-added.

During this time the [redacted] specialist had discussions with a specialist from the [redacted] ([redacted]) group. Together they mistakenly concluded that no NERC work/documentation was needed for this action.

The module was programmed using the corporate computer used by the SME, which is also a designated TCA. The SME did not capture the evidence that the TCA had all the controls on. Hence a violation of CIP010 R4.

A [redacted] at [redacted] learned of this occurrence of non-compliance with the TCA process on October 23 and submitted a Potential Violation Notification

Individuals at [redacted] connected to the NERC-CIP assets with transient devices and not following the "[redacted]" program to collect appropriate evidence of compliance.

Lack of understanding at [redacted] for working with TCA's. This resulted in the SME's not following the [redacted]" procedure.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017018761 Certification Package	CIP-010-2 R4
File 2	RFC2017018761 Updated Evidence for Milestone 1	CIP-010-2 R4
File 3	RFC2017018760 Milestone 3 Submit	CIP-010-2 R4
File 4	RFC2017018761 Milestone 2 Additional Evidence	CIP-010-2 R4

Verification of Mitigation Plan Completion

Milestone 1: Conduct training for all the [redacted] SME's about the TCA process.

Proposed Completion Date: November 3, 2017

Actual Completion Date: February 6, 2018

File 2, "*RFC2017018761 Update Evidence for Milestone 1*", Pages 1 through 4, show the required SMES who need to be trained on the TCA process/procedure, the [redacted] (Training System) output as to who had completed the training and when.

Milestone # 1 Completion verified.

Milestone 2: Prepare a change order and run a new baseline to contain the violation.

Proposed Completion Date: December 22, 2017

Actual Completion Date: December 19, 2017

File 1, "*RFC2017018761 Certification Package*", Milestone 2- Submit, Pages 2 and 3, show one set of baseline information. This can be paired with File 4, "*RFC2017018761 Milestone 2- Additional Evidence*", Pages 2, showing baselines from February 16, 2016, compared to a baseline taken from December 19, 2017.

Milestone # 2 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: April 11, 2018

Anthony Jablonski
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Attachment 16

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

16.a The Entity's Self-Report (RFC2017017838);
16.b The Entity's Mitigation Plan designated as RFCMIT013012 submitted [redacted];
16.c The Entity's Certification of Mitigation Plan Completion dated [redacted];
16.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted]

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-011-2
Requirement: CIP-011-2 R1.
Date Submitted: [redacted]
Has this violation previously been reported or discovered?: No

Entity Information:

Joint Registration Organization (JRO) ID:
Coordinated Functional Registration (CFR) ID:
Contact Name: [redacted]
Contact Phone: [redacted]
Contact Email: [redacted]

Violation:

Violation Start Date: July 01, 2016 **Changed to December 1, 2016**
End/Expected End Date:
Reliability Functions: [redacted]
Is Possible Violation still occurring?: No
Number of Instances: 1
Has this Possible Violation been reported to other Regions?: No
Which Regions:
Date Reported to Regions:

Detailed Description and Cause of Possible Violation:

*Detailed Description:
From December 2016 through February 2017, [redacted] upgraded to [redacted] This version had a default setting for file saves to [redacted] a [redacted] based storage. On 4/17/2017, the [redacted] Prevention ([redacted] tool was used by [redacted] ([redacted] to scan [redacted] and [redacted] for BES Cyber System Information (BCSI) labeled documentation in the [redacted] The scan searched for files with the phrases '[redacted] Information" and '[redacted] Confidential". The scan found [redacted] instances of BCSI documentation stored on [redacted] locations and two (2) test documents on [redacted] Out of [redacted] instances of BCSI documentation identified by the [redacted] tool, only [redacted] contained BCSI. The BCSI contained in these [redacted] document was [redacted] and [redacted] is a [redacted] only instance with access to [redacted] personnel only. Each individual has his/her own [redacted] like a personal drive. An individual cannot see information on another personal drive. As it is not a [redacted] defined storage and BCSI was stored, this created a violation of CIP-011 R1 P1.1. We further verified that the documents that were stored prior to enabling [redacted] (4/17/17) could only be accessed by the owner and those documents were quarantined immediately by the tool, therefore no one could access those documents after the detection. All [redacted] copies were deleted from [redacted] by 6/22/2017.

*Root Cause of Possible Violation:
The operating system upgrade process did not include an assessment of the

potential impact of change in default save settings. Training materials or guidance documents regarding appropriate use of the [redacted] were not made available to employees.

*How was the violation discovered?
Violation was discovered when the [redacted] tool was turned on to scan for sensitive or critical information outside the corporate network.

*Timeline:
1. December 2016 - [redacted] began transition to [redacted]
2. April 17, 2017 - The [redacted] was turned on.
3. April 17, 2017 - The [redacted] BCSI documents were removed from the [redacted] storage location.
4. April 27, 2017 - [redacted] notified of the Possible Non-Compliance.
5. May 3, 2017 - An [redacted] was conducted.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Only the owner of the file could access the file stored on [redacted]
All [redacted] BCSI documents were contained in designated secured BCSI storage location after once identification by the [redacted] scan. [redacted] documents containing BCSI were deleted by 6/22/2017.
Continue implementation of the [redacted] tools to verify that BCSI documents are not stored in the [redacted] or [redacted] location. [redacted] will make sure that end users do not send sensitive or critical information outside the corporate network.
Change the default setting for [redacted] to prevent reoccurrence.
Revise Communication Plan for the [redacted] program rollout of [redacted] and [redacted] to [redacted] employees with language that NERC BCSI storage in these locations is prohibited.

Preventive Measures:
• [redacted] will communicate across Business Units that the use of storage locations not identified as BCSI storage locations for BSCI documents is prohibited based on our CIP011 R1 P1.1 Information Protection Program.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Minimal

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS:

The Potential Impact to the BES is low because the [redacted] BCSI documentations could be accessed only the by the owner of the file.

The Actual Impact to the BES is none because the documents have been contained and [redacted] has experienced no negative impact to its Bulk Electric System.

Risk Assessment of Impact to BPS:

[redacted] identifies that that potential impact to the BES is low. [redacted] has not identified any negative impact to its Bulk Electric System assets as a result of this potential violation.

Additional Entity Comments:

Self Report

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code: RFCMIT013012

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017017838	CIP-011-2 R1.	

Mitigation Plan Submitted On: [redacted]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: June 30, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

(1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
(2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
(3) The cause of the Alleged or Confirmed Violation(s).
(4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
(5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
(6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
(7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
(8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
(9) Any other information deemed necessary or appropriate.
(10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
(11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

• The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.

• This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.

• If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.

• Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.

• Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.

• The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [redacted]

NERC Compliance Registry ID: [redacted]

Address: [redacted]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [redacted]

Title: [redacted]

Email: [redacted]

Phone: [redacted]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017017838	07/01/2016	CIP-011-2 R1.
Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1 – Information Protection.		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

From December 2016 through February 2017, [redacted] upgraded to [redacted] This version had a default setting for file saves to [redacted] a [redacted] based storage. On 4/17/2017, the [redacted] Prevention ([redacted] tool was used by [redacted] ([redacted] to scan [redacted] and [redacted] for BES Cyber System Information (BCSI) labeled documentation in the [redacted] The scan searched for files with the phrases '[redacted] Information" and '[redacted] Confidential". The scan found [redacted] instances of BCSI documentation stored on [redacted] locations and two (2) test documents on [redacted] Out of [redacted] instances of BCSI documentation identified by the [redacted] tool, only [redacted] located on [redacted] contained BCSI. The two documents on [redacted] were reviewed and determined as not BCSI Documents. The BCSI contained in these [redacted] documents consisted of [redacted] and [redacted] and [redacted] are a [redacted] only instance with access by [redacted] personnel only. Each has their own [redacted] and [redacted] like a personal drive. An individual cannot see information on another personal drive. As it is not a [redacted] defined storage and BCSI was stored, this created a violation of CIP-011 R1 P1.1. We further verified that the documents that were stored prior to enabling [redacted] (4/17/17) could only be accessed by the owner and those documents were quarantined immediately by the tool, therefore no one could access those documents after the detection. All [redacted] copies were deleted from [redacted] by 6/22/2017. Furthermore, [redacted] configured [redacted] tool to monitor and quarantined in near real time NERC-CIP Documents for all on going activities on [redacted] and [redacted]
Cause of Possible Violation:

The operating system upgrade process did not include an assessment of the potential impact of change in default save settings. Training materials or guidance documents regarding appropriate use of the [redacted] were not made available to employees.

Timeline:
December 2016 - [redacted] began transition to [redacted]
April 17, 2017 - The [redacted] tool was turned on.
April 17, 2017 - The [redacted] BCSI documents were removed from the [redacted] storage location.
April 27, 2017 - [redacted] notified of the Possible Non-Compliance.
May 3, 2017 - An [redacted] was conducted.
June 22, 2017 - All BCSI documents that were in [redacted] and [redacted] were deleted.

What is the violation?

The [redacted] tool was enabled by [redacted] to scan [redacted] and [redacted] in the [redacted] for BCSI labeled documentation. The final report included [redacted] instances of BCSI documentation stored in [redacted] and [redacted] locations that violates CIP-011 R1 P1.1.

Relevant information regarding the identification of the violation(s):

Violation was discovered when the [redacted] tool was turned on to scan for sensitive or critical information outside the corporate network.

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

Milestone 1: The intended outcome is to monitor for and quarantine NERC CIP documents uploaded to [redacted] and [redacted] The evidence is a completed work order and screen shot of the [redacted] policy.

Milestone 2: Update the NERC CIP Information Identification Classification, and Protection Program to state that storage on [redacted] and [redacted] is prohibited. The evidence shows the program updates were completed.

Milestone 3: The intended outcome is a distributed communication about [redacted] and [redacted] to [redacted] Employees with language that NERC BCSI storage in these locations is prohibited. The evidence shows the distributed email communication.

Milestone 4: The intended outcome is to verify if any files in [redacted] and [redacted] are BCSI documents and if so, are removed or deleted. This will be measured through the [redacted] scans. The evidence shows an email by the SMEs verifying that those files were identified as BCSI documents and were removed or deleted from [redacted] and [redacted]

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: June 30, 2017

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
[redacted] tool configuration	[redacted] is configured to near real time monitor for and quarantine NERC CIP documents.	04/11/2017	04/11/2017		No
Update the NERC CIP Information Identification, classification, and Protection Program	Update the NERC CIP Information Identification Classification, and Protection Program to state that storage on [redacted] and [redacted] is prohibited.	04/17/2017	04/17/2017		No
Communication about prohibition of BCSI on [redacted] across Business	Communication across [redacted] about update to the	05/22/2017	05/22/2017		No

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Units ([redacted]	Information Identification Classification, and Protection Program that storage on [redacted] and [redacted] is prohibited.				
Remove BCSI documents found on [redacted]	An email by SMEs verifying that files identified as BCSI have been removed or deleted from [redacted] and [redacted]	06/30/2017	06/23/2017		No

Additional Relevant Information

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

The Potential Impact to the BES is low because the [redacted] BCSI documentations could be accessed only the by the owner of the file.

The Actual Impact to the BES is none because the documents have been contained and [redacted] has experienced no negative impact to its Bulk Electric System.

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

By completion of the mitigation plan [redacted] will minimize similar issues from occurring. Milestone 1 will enable [redacted] tool policies to monitor for and quarantine files with BCSI. Milestone 2 will update the NERC CIP Information Identification Classification, and Protection Program to state that storage on [redacted] and [redacted] is prohibited. Milestone 3 is communication rollout to [redacted] Employees with language that NERC BCSI storage in [redacted] and [redacted] locations is prohibited. Milestone 4 will verify if the files in [redacted] and [redacted] are BCSI documents, and if there, are then removed or deleted.

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

Acknowledges:

1. I am qualified to sign this mitigation plan on behalf of my organization.

2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.

3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

[redacted] Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name: [redacted]

Title: [redacted]

Authorized [redacted]

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

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request 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)

Registered Entity Name: [redacted]
NERC Registry ID: [redacted]
NERC Violation ID(s): RFC2017017838
Mitigated Standard Requirement(s): CIP-011-2 R1.
Scheduled Completion as per Accepted Mitigation Plan: June 30, 2017
Date Mitigation Plan completed: June 30, 2017
RF Notified of Completion on Date: [redacted]
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017838 Certification Package.zip	File "RFC2017017838 Certification Package.Zip" contains the cover page for the package and also the supporting documents for each milestone.	1,392,937

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [redacted]
Title: [redacted]
Email: [redacted]
Phone: [redacted]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Mitigation Plan Verification for RFC2017017838

[redacted]

Standard/Requirement: CIP-011-2 R1

NERC Mitigation Plan ID: RFCMIT013012

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report [redacted]	[redacted]	[redacted]		[redacted]	06/30/17

Description of Issue

From December 2016 through February 2017, [redacted] upgraded to [redacted] This version had a default setting for file saves to [redacted] a [redacted] based storage. On 4/17/2017, the [redacted] tool was used by [redacted] to scan [redacted] and [redacted] for BES Cyber System Information (BCSI) labeled documentation in the [redacted] The scan searched for files with the phrases "[redacted] Information" and "[redacted] Confidential". The scan found [redacted] instances of BCSI documentation stored on [redacted] locations and [redacted] test documents on [redacted] Out of [redacted] instances of BCSI documentation identified by the [redacted] tool, only [redacted] located on [redacted] contained BCSI. The [redacted] documents on [redacted] were reviewed and determined as not BCSI Documents. The BCSI contained in these [redacted] documents consisted of [redacted] and [redacted] and [redacted] are a [redacted] only instance with access by [redacted] personnel only. Each has their own [redacted] and [redacted] like a personal drive. An individual cannot see information on another personal drive. As it is not a [redacted] defined storage and BCSI was stored, this created a violation of CIP-011 R1 P1.1. We further verified that the documents that were stored prior to enabling [redacted] (4/17/17) could only be accessed by the owner and those documents were quarantined immediately by the tool, therefore no one could access those documents after the detection. All [redacted] copies were deleted from [redacted] by 6/22/2017. Furthermore, [redacted] configured [redacted] tool to monitor and

quarantined in near real time NERC-CIP Documents for all on going activities on [redacted] and [redacted]

Cause of Possible Violation: The operating system upgrade process did not include an assessment of the potential impact of change in default save settings. Training materials or guidance documents regarding appropriate use of the [redacted] were not made available to employees.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017017838 Certification Package	CIP-011-2 R1

Verification of Mitigation Plan Completion

Milestone 1: [redacted] tool configuration

File 1, "*RFC2017017838 Certification Package*", Milestone 1- Submit, Pages 3 through 5, show the approved change control ticket that was utilized in order to reconfigure the entity [redacted] Pages 7 through 15 show the configuration changes that were made to [redacted] in order to meet this milestone.

Milestone # 1 Completion verified.

Milestone 2: Update the NERC CIP Information Identification, classification, and Protection Program

File 1, "*RFC2017017838 Certification Package*", Milestone 2- Submit, Page 5, show the update to the entity BCSI storage documentation re-affirming that no BCSI should be stored in certain entity locations [redacted] or [redacted].

Milestone # 2 Completion verified.

Milestone 3: Communication about prohibition of BCSI on [redacted] across [redacted] ([redacted]

File 1, "*RFC2017017838 Certification Package*", Milestone 3- Submit, Pages 2 and 3, show the communications surrounding the changes to the entity procedures in regards to storing of NERC CIP classified information.

Milestone # 3 Completion verified.

Milestone 4: Remove BCSI documents found on [redacted]

File 1, "*RFC2017017838 Certification Package*", Milestone 4- Submit, Pages 2 through 20, show the communications from members of departments stating that scans were run and BCSI was removed from unauthorized repositories.

Milestone # 4 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: [redacted]

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation