Attachment 4

Record documents for the violation of CIP-003-3 R6

4.a The Entity's Self-Report (RFC2017017568);
4.b The Entity's Mitigation Plan designated as RFCMIT012980 submitted [redacted];
4.c The Entity's Certification of Mitigation Plan Completion dated [redacted];
4.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted];
4.e The Entity's Self-Report (RFC2017018261);
4.f The Entity's Mitigation Plan designated as RFCMIT013213-1 submitted [redacted];
4.g The Entity's Certification of Mitigation Plan Completion dated [redacted];
4.h ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted];
4.i The Entity's Self-Report (RFC2017018760);
4.j The Entity's Mitigation Plan designated as RFCMIT013443 submitted [redacted];
4.k The Entity's Certification of Mitigation Plan Completion dated [redacted];
4.l ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted]

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-004-6
Requirement: CIP-004-6 R4.
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: May 08, 2017 **Changed to November 10, 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 11/10/2016 [redacted] responsible for administering access security, assigned [redacted] 1 and 2 to a supervisor in [redacted] without following the NERC [redacted] process that requires an approval from the leader. These [redacted] grants access to vendor [redacted] to remote access [redacted] When vendor need to remote login, vendor calls [redacted] group who in turn verifies that vendor calling is [redacted] authorized user, and assigns the [redacted] passcode to complete dual authentication. [redacted] The [redacted] process is an access control management system which hold the record of authorized access for [redacted] employees and contractors. [redacted] appliance is classified as an [redacted] for [redacted] assets. This unauthorized access was identified on 3/3/2017 during the [redacted] to [redacted] process. This [redacted] process compares authorized access with provisioned access. This provisioning without following process to authorize access violates CIP-004 R4.1. "Process to authorized based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances"

*Root Cause of Possible Violation:
Then NERC [redacted]

process was not followed.

*How was the violation discovered?
Violation was identified during the 2017 Q1 [redacted] to [redacted] process.

*Timeline:
November 10, 2016 - [redacted] received an email (NOT [redacted] authorization) from an employee of [redacted] who is not a formal leader to grant access to [redacted] 1 and 2 to the supervisor of [redacted]
November 10, 2016 - [redacted] assigned [redacted] to an employee without [redacted] authorization approvals.
March 3, 2017 - An internal review of data for CIP004 R4.1 identified the provisioned access without [redacted] authorization approvals.
March 24, 2017 - After completion of [redacted] process, [redacted] was notified of Potential Violation.
March 31, 2017 - [redacted] and RCA was conducted.
May 3, 2017 - [redacted] 1 and 2 assigned to the employee were revoked.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: The [redacted] ownership were changed May 3, 2017. After ownership changes the [redacted] code has disabled status and is no longer useable. The [redacted] process will be communicated to every leader with NERC CIP access employees.

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: As per VSL, the potential impact is severe.

Actual Impact: The actual impact to the BES is low. [redacted] has experienced no negative impact to its Bulk Electric System assets as a result of this potential violation.

Risk Assessment of Impact to BPS: No actual impact to BES has been noted due to this 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:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017017568	CIP-004-6 R4.	

Mitigation Plan Submitted On: [redacted]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: July 28, 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		
RFC2017017568	05/08/2017	CIP-004-6 R4.
Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.		

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

Brief Description: (What happened?)

On 11/10/2016 [redacted] responsible for administering access security, assigned [redacted] 1 and 2 to a supervisor in [redacted] group without following the [redacted] process that requires an approval from the leader. These [redacted] grant access to the vendor [redacted] to remote access [redacted] When the vendor needs to remote login, the vendor calls the [redacted] group who in turn verifies that the vendor calling is [redacted] authorized user, and assigns the [redacted] passcode to complete dual authentication. [redacted] The [redacted] process is an access control management system that holds the record of authorized access for [redacted] employees and contractors. [redacted] appliance is classified as an EACMS for [redacted] assets.
This unauthorized access was identified on 3/3/2017, during the 2017 Q1 [redacted] to [redacted] process. This [redacted] process compares authorized access with provisioned access. This provisioning without following process to authorize access violates CIP-004 R4.1. "Process to authorized based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances"

Cause: (what caused the violation?)

The NERC [redacted] process was not followed.

Timeline:

November 10, 2016 - [redacted] received an email (NOT [redacted] authorization) from an employee of [redacted] who is not a formal leader to grant access to [redacted] 1 and 2 for the supervisor of [redacted]
November 10, 2016 - [redacted] assigned [redacted] to an employee without [redacted] authorization approvals.
March 3, 2017 - An internal review of data for CIP004 R4.1 identified the provisioned access without [redacted] authorization approvals.
March 24, 2017 - After completion of [redacted] process, [redacted] was notified of Potential Violation.
March 31, 2017 - [redacted] and RCA was conducted.
May 3, 2017 - [redacted] 1 and 2 assigned to the employee were revoked.

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

Violation was identified during the 2017 Q1 [redacted] to [redacted] process.

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. Milestone 1 will provide evidence showing access has been revoked for [redacted] 1 and 2.
2. Milestone 2 will show that a disciplinary action has been taken to correct the employee behavior.
3. Milestone 3: Update procedures to indicate that the leader must approve reassignment of [redacted]
4. Milestone 4: Update job aid to identify [redacted] as NERC-CIP asset when assigning to the owner.

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: July 28, 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
Revoke Access	Evidence showing access has been revoked for [redacted] 1 and 2.	05/03/2017	05/03/2017		No
Disciplinary Action	Disciplinary Action	06/14/2017	06/14/2017		No
Job aid Update	Update job aid to identify [redacted] as NERC-CIP asset when assigning to the owner.	07/28/2017			No
Procedure update	Update procedures to indicate that the leader must approve reassignment of [redacted]	07/28/2017			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.

By implementing the mitigation plan proposed in section D, [redacted] will minimize similar issues. The disciplinary action is designed to correct the employee's behavior.

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. The disciplinary action is designed to correct the employee's behavior.

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]

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): RFC2017017568
Mitigated Standard Requirement(s): CIP-004-6 R4.
Scheduled Completion as per Accepted Mitigation Plan: July 28, 2017
Date Mitigation Plan completed: July 28, 2017
RF Notified of Completion on Date: [redacted]
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017568 Certification package.zip		1,382,946

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 RFC2017017568

[redacted]

Standard/Requirement: CIP-004-6 R4

NERC Mitigation Plan ID: RFCMIT012980

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]	07/28/17

Description of Issue

On 11/10/2016, a [redacted] responsible for administering access assigned [redacted] 1 and 2 to a supervisor in the [redacted] group without following the NERC [redacted] process that requires an approval from the leader. These [redacted] grant access to the vendor [redacted] to remote access [redacted]

This unauthorized access was identified on 3/3/2017 during the 2017 Q1 [redacted] to [redacted] process.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017017568 Certification Package	CIP-004-6 R4

Verification of Mitigation Plan Completion

Milestone 1: Revoke Access.

File 1, "*RFC2017017568 Certification Package*", [redacted] 1 and 2 access removal as evidence showing access has been revoked for [redacted] 1 and 2.

Milestone # 1 Completion verified.

Milestone 2:

File 1, "*RFC2017017568 Certification Package*", Disciplinary Action Email as evidence of an email by Employee Relation stating a corrective action was taken June 14, 2017, for the employee.

Milestone # 2 Completion verified.

Milestone 3: Job aid Update.

File 1, "*RFC2017017568 Certification Package*", [redacted] as evidence that shows an update has been made for a job aid stating that [redacted] will be identified as a NERC-CIP asset when assigning to the owner. [redacted] also provided an email communication as evidence an email was sent to subject matter experts that the [redacted] job aid has been modified/updated.

Milestone # 3 Completion verified.

Milestone 4: Procedure update.

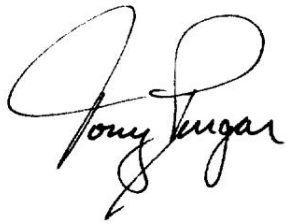
File 1, "*RFC2017017568 Certification Package*", Leader Approve of [redacted] as evidence that shows an update has been made for a job aid stating that the leader must approve reassignment of the [redacted] It was noted in the mitigation plan that a procedure will be updated. However, [redacted] made the update to the job aid. [redacted] also provided an email communication as evidence

an email was sent to subject matter experts that the [redacted] aid has been modified/updated.

Milestone # 4 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-004-6

Requirement: CIP-004-6 R4.

Date Submitted: August 18, 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: January 12, 2017 **Changed to January 13, 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 Monday, 06/19/2017, during the Q2 [redacted] and SME training session of the [redacted] to [redacted] process it was identified that [redacted] users with [redacted] had access to [redacted] Configuration Items (NERC-CIP), abbreviated within this document as [redacted] CI, BES Cyber System Information (BCSI) without a corresponding authorization record, a CIP 004 part 4.4 potential violation, in [redacted]
The [redacted] CI application is an application within the [redacted] of applications that [redacted] uses to store the BES Cyber System List. [redacted] is the application that holds the authorization records for users with access to NERC CIP assets and BCSI. At least quarterly [redacted] uses the [redacted] to [redacted] process to validate that all authorized users have corresponding authorization records in [redacted]
The summary of access privileges at the time were 10 [redacted] users with [redacted] and [redacted] users with [redacted].
The specific breakdown of entitlements was as follows:
[redacted] users:
One of the users was an [redacted] manager had the entitlement [redacted] NERC, which gives the user administrator privileges to read, write, and delete BCSI information in [redacted] CI.
Nine users had the entitlement, [redacted] NERC, which gives the user administrator privileges to read, write, and delete BCSI information in [redacted]

Self Report

CI.
Of these [redacted] users with access to [redacted] assets, [redacted] of the employees are [redacted] application system administrators. Their administrative privileges are adopted when they build new applications within [redacted]

[redacted] users with [redacted] entitlements:
A breakdown of the users with access to [redacted] assets is as follows:
• [redacted]

See attachment "Description of entitlements.docx"
On 7/7/2017, the SME in training that identified the potential non-compliance notified the [redacted] of the potential non-compliance.
On 7/13/2017, [redacted] performed an [redacted] where the root cause of the potential violation was determined to be a breakdown of process within the [redacted] Requests for Access process. [redacted] did not have a process step identified in the [redacted] Requests for Access process that required a validation of [redacted] authorization records after the completion of bulk access provisioning. The [redacted] Requests for Access process was updated 7/1/17 to address this gap.
It was also identified that on 1/12/2017, prior to the creation of the current [redacted] bulk upload process (created 03/01/2017), a request to bulk load [redacted] employees into [redacted] CI using the [redacted] Requests for Access process was sent to the access management team. [redacted] Access was granted to each user on 01/13/2017, however there was no requirement in the [redacted] Requests for Access process to validate authorization records were present in [redacted]
The actions resulting from that [redacted] were to contain or correct the possible non-compliance by completing the bulk load process for the [redacted] users, determine the extent of conditions by further investigating user access rights for the [redacted] users, and to prevent any future potential non-compliance by updating the [redacted] Requests for Access procedure to validate [redacted] authorization records are present after the completion of the bulk loading provisioning process.
On 7/20/2017, in an effort to contain the potential non-compliance, [redacted] attempted to bulk upload the [redacted] users into [redacted] when it was identified that [redacted] out of the [redacted] and [redacted] users impact users did not hold one or more of the proper qualifications (need, NERC CIP Training, Personal Risk Assessment (PRA)) for BCSI access.
[redacted] user, employee [redacted], did not have current NERC CIP training which is a potential noncompliance of CIP004 part 2.2. This employee did not maintain any physical access to any [redacted] assets or sites.
[redacted] users, [redacted], did not maintain current NERC CIP training or have a valid PRA which is a potential noncompliance of CIP004 part 2.2 and part 3.2. However, these employees did not maintain any physical access to any [redacted] assets or sites.
On 07/21/2017 BCSI access to [redacted] CI was removed for all 1 high/medium

Self Report

impact user and [redacted] users to contain the possible non-compliance.
On 07/27/2017 a [redacted] was initiated on the 16 users to verify that all access is accurate.
On 08/04/2017 the [redacted] was completed resulting in the removal of access for one (1) [redacted] user, [redacted] The access for this employee was identified as no longer appropriate.
*Root Cause of Possible Violation: There was no process step within the [redacted] Request for Access process requiring a validation of access entitlements in [redacted] after completing a bulk load of access during the [redacted] Requests for Access process.
*How was the violation discovered? During the Q2 [redacted] and SME training session of the [redacted] to [redacted] process it was identified that [redacted] users with [redacted] entitlements had access to [redacted] (NERC) BES Cyber System Information (BCSI) without a corresponding authorization record in [redacted]
*Timeline:
1-12-17 [redacted] Request for Access Bulk load for [redacted] employees
3-1-17 [redacted] Bulk load process created
6-19-17 Q2 [redacted] to [redacted] Process conducted and potential violation identified. This is the first [redacted] the [redacted] CI application was included in the [redacted] since implementation on 02-09-2017.
7-7-17 Potential violation reported to [redacted]
7-13-17 [redacted] conducted
7-20-17 Bulk load of [redacted] employees attempted
7-21-17 Removal of access for [redacted] employees
7-27-17 [redacted] initiated
8-4-17 [redacted] complete and [redacted] employee access removed

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Mitigating Activities:
[redacted] attempted to load all [redacted] users using the current bulk load process into [redacted] on 07-20-17. [redacted] then removed [redacted] employees due to qualification gaps on 7-21-17. [redacted] conducted a [redacted] for [redacted] employees to verify access on 7-27-17. [redacted] removed access for [redacted] employee on 8-4-17 due to the employee no longer requiring access.

Preventative Measures:
On 03/01/17 [redacted] implemented an [redacted] bulk load process that addressed how to properly load access qualifications into [redacted] On 7-1-17 [redacted] revised the [redacted] Request for Access Standard Work Instruction (SWI) to include a requirement to verify in [redacted] that prior to conducting a bulk load to validate that all users have been bulk loaded into [redacted]

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: As per the VSL table and the potential impact to the BES is Lower because [redacted] users gained access without the proper qualifications.

The actual impact is low due to compensating controls of the [redacted] that worked as designed to catch any inaccurate access. Additionally, [redacted] users maintained all qualification required to have access to the BCSI.

Risk Assessment of Impact to BPS: The risk of the Impact to the BES is low due to the compensating controls of the [redacted] and the removal of access of the [redacted] employees without proper

Self Report

access qualifications and the 1 removal of access for the employee that no longer required access.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Description of Entitlements.docx	This file contains description of entitlements noted in this violation.	13,052

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code: RFCMIT013213-1

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
RFC2017018261	CIP-004-6 R4.	

Mitigation Plan Submitted On: October 17, 2017

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: August 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		
RFC2017018261	01/12/2017	CIP-004-6 R4.
Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.		

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

[redacted] Processes
When loading multiple users into an application [redacted] uses a bulk loading method. The process requires that first users must be loaded in to the [redacted] ([redacted] which is [redacted] system that retains authorization records. Then users are loaded into the application using the [redacted] Request for Access process. This process is used to load user access right into an application.
[redacted] also uses a [redacted] process that is used to verify that any access granted is appropriate access for each user. The process requires each role owner and supervisor to review the access of the users they are responsible for and respond if access is appropriate for the user. If either the role owner or the supervisor believes that the access is no longer appropriate the users access will be removed. [redacted] may use this process following any load of user access.

On Monday, 06/19/2017, during the Q2 [redacted] ([redacted] and SME training session of the [redacted] to [redacted] process it was identified that [redacted] had access to [redacted] Configuration Items (NERC-CIP), abbreviated within this document as [redacted] CI, BES Cyber System Information (BCSI) without a corresponding authorization record, a CIP 004 part 4.4 potential violation, in [redacted] ([redacted]
The [redacted] CI application is an application within the [redacted] Suite of applications that [redacted] uses to store the BES Cyber System List. [redacted] is the application that holds the authorization records for users with access to NERC CIP assets and BCSI. At least quarterly [redacted] uses the [redacted] to [redacted] process to validate that all authorized users have corresponding authorization records in [redacted]
The summary of access privileges at the time were [redacted] users with [redacted] and [redacted] users with [redacted]
The specific breakdown of entitlements was as follows:
[redacted] users:
[redacted]
Of these [redacted] users with access to [redacted] assets, [redacted] of the employees are [redacted] application system administrators. Their administrative privileges are adopted when they build new applications within [redacted]
[redacted] users with [redacted]:
[redacted]

See attachment "Description of entitlements.docx"
On 7/7/2017, the SME in training that identified the potential non-compliance and notified the [redacted] of the potential non-compliance.
On 7/13/2017, [redacted] performed an [redacted] where the root cause of the potential violation was determined to be a breakdown of process within the [redacted] Requests for Access process. [redacted] did not have a process step identified in the [redacted] Requests for Access process that required a validation of [redacted] authorization records after the completion of bulk access provisioning. The [redacted] Requests for Access process was updated 8/1/17 to address this gap.
It was also identified that on 1/12/2017, prior to the creation of the current [redacted] bulk upload process (created 03/01/2017), a request to bulk load [redacted] identified employees into [redacted] CI using the [redacted] Requests for Access process was sent to the access management team. [redacted] Access was granted to each user on 01/13/2017, however there was no requirement in the [redacted] Requests for Access process to validate authorization records were present in [redacted]
The actions resulting from that [redacted] were to contain or correct the possible non-compliance by completing the bulk load process for the [redacted] users, determine the extent of conditions by further investigating user access rights for the [redacted] and to prevent any future potential non-compliance by updating the [redacted] Requests for Access procedure to validate [redacted] authorization records are present after the completion of the bulk loading provisioning process.
On 7/20/2017, to contain the potential non-compliance, [redacted] attempted to bulk upload the [redacted] users into [redacted] when it was identified that [redacted] high/medium and [redacted] out of the [redacted] users impact users did not hold one or more of the proper qualifications (need, NERC CIP Training, Personal Risk Assessment (PRA)) for BCSI access.
[redacted] user, [redacted] did not have current NERC CIP training which is a potential noncompliance of CIP004 part 2.2. This employee did not maintain any physical access to any [redacted] assets or sites.
[redacted] users, [redacted], did not maintain current NERC CIP training or have a valid PRA which is a potential noncompliance of CIP004 part 2.2 and part 3.2. However, these employees did not maintain any physical access to any [redacted] assets or sites.
On 07/21/2017 BCSI access to [redacted] CI was removed for all [redacted] user and [redacted] users to contain the possible non-compliance.
On 07/27/2017 prior to the implementation of the new process step within the [redacted] Request for Access SWI, a [redacted] was initiated on the [redacted]. [redacted] required that a [redacted] be conducted on the users being bulk uploaded to verify that all users that were granted access continued to require access.
On 08/01/2017, [redacted] instituted a new process step within the [redacted] Request for Access SWI that requires the SME to validate, prior to performing a bulk load users in application, that there are proper role owner approvals and that all users have been loaded into [redacted] is [redacted] system that holds authorization records for each user.

On 08/04/2017 the [redacted] was completed resulting in the removal of access for [redacted] user, employee [redacted] The access for this employee was identified as no longer appropriate.
Cause: (what caused the violation?)
During the load of [redacted] employees access into [redacted] (NERC) there was no check to determine if each employee maintained access records in [redacted]

How was the violation discovered?

During the Q2 [redacted] and SME training session of the [redacted] to [redacted] process it was identified that [redacted] entitlements had access to [redacted] (NERC) BES Cyber System Information (BCSI) without a corresponding authorization record in [redacted]

Results of the RCA: (What is the root cause?)
There was no process step within the [redacted] Request for Access process requiring a validation of access entitlements in [redacted] after completing a bulk load of access during the [redacted] Requests for Access process.

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

This potential non-compliance was identified by [redacted] during the Q2 [redacted] On 03/01/2017, prior to the identification of this potential non-compliance, [redacted] documented and updated its [redacted] process to address process gaps when bulk loading employees access records.

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:

Mitigating Activities:
[redacted] attempted to load all [redacted] users using the current bulk load process into [redacted] on 07-20-17. On 07-21-17, [redacted] then removed [redacted] employees due to qualification gaps identified during that bulk load. [redacted] conducted a [redacted] for [redacted] employees to verify access on 07-27-17. [redacted] conducted a [redacted] for the [redacted] users to ensure that all access was still needed. The [redacted] resulted in the removal of [redacted] employee on 8-4-17 due to the employee no longer requiring access. The intent of this action was to bring [redacted] back into compliance with CIP 004 part 4.4.
Preventative Measures:
On 03-01-17, prior to the identification of this potential non-compliance, [redacted] documented and updated the [redacted] bulk load process that addressed how to properly load access qualifications into [redacted] On 8-1-17 [redacted] revised the [redacted] Request for Access Standard Work Instruction (SWI) to include a requirement to verify in [redacted] that prior to conducting a bulk load to validate that all users have been bulk loaded into [redacted] The intent of this action is to prevent granting access to BCSI without proper qualification and without a matching authorization record.

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: August 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
Document [redacted] bulk load process	Document and update the [redacted] bulk load process	03/01/2017	03/01/2017		No
90 days check	Purpose of this milestone is a 90 check on the progress of the milestone. No evidence is provided for this milestone.	06/01/2017	06/01/2017		No
Conduct bulk upload into [redacted]	Conduct bulk upload for [redacted] users into [redacted] and identify any users without proper access qualifications	07/20/2017	07/20/2017		No
Remove access	Remove access to [redacted] employees with	07/21/2017	07/21/2017		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
	missing qualification				
Update the [redacted] Request for access SWI	Update the [redacted] Request for access SWI to require validation that users are loaded into [redacted] prior to performing bulk load	08/01/2017	08/01/2017		No
Conduct a [redacted] of access	Conduct a [redacted] for the [redacted] employees with missing authorization records and remove any inappropriate access	08/30/2017	08/04/2017		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 Lower because [redacted] users gained access without the proper qualifications. The actual impact is low due to compensating controls of the [redacted] that worked as designed to catch any inaccurate access. Additionally, [redacted] users maintained all qualification required to have access to the BCSI. [redacted] removed access to the users without proper qualification along with conducting an off-cycle [redacted] to validate if access was needed for each employee identified in this potential non-compliance.

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 completion of the Mitigation Plan as outlined and implemented will help to ensure that during user access bulk uploads all users access is provisioned properly and that all users access has a corresponding authorization record.

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: October 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): RFC2017018261
Mitigated Standard Requirement(s): CIP-004-6 R4.
Scheduled Completion as per Accepted Mitigation Plan: August 30, 2017
Date Mitigation Plan completed: August 04, 2017
RF Notified of Completion on Date: October 27, 2017
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017018261 Certification Package.zip	File "RFC2017018261 Certification Package.zip" contains the coversheet and supporting evidence for each milestone.	3,604,426

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 RFC2017018261

[redacted]

Standard/Requirement: CIP-004-6 R4

NERC Mitigation Plan ID: RFCMIT013213-1

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 08/18/17	10/17/17	10/23/17	11/02/17	10/27/17	08/04/17

Description of Issue

When loading multiple users into an application [redacted] uses a bulk loading method. The process requires that first users must be loaded in to the [redacted] which is [redacted] system that retains authorization records. Then users are loaded into the application using the [redacted] Request for Access process. This process is used to load user access right into an application.

[redacted] also uses a [redacted] process that is used to verify that any access granted is appropriate access for each user. The process requires each role owner and supervisor to review the access of the users they are responsible for and respond if access is appropriate for the user. If either the role owner or the supervisor believes that the access is no longer appropriate the users access will be removed. [redacted] may use this process following any load of user access.

On Monday, 06/19/2017, it was identified that [redacted] entitlements had access to [redacted] Configuration Items (NERC-CIP), BES Cyber System Information (BCSI) without a corresponding authorization record.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017018261 Certification Package	CIP-004-6 R4

Verification of Mitigation Plan Completion

Milestone 1: Document [redacted] bulk load process.

Proposed Completion Date: March 1, 2017

Actual Completion Date: March 1, 2017

File 1, "*RFC2017018261 Certification Package*", Document [redacted] bulk upload process-RFC2017018261, Pages 1 through 7, shows the documented procedure for [redacted] bulk upload and when it is to be used Vs. manual addition to [redacted]

Milestone # 1 Completion verified

Milestone 2: 90 days check.

Proposed Completion Date: June 1, 2017

Actual Completion Date: June 1, 2017

No evidence required as milestone is filler.

Milestone # 2 Completion verified

Milestone 3: Conduct bulk upload into [redacted]

Proposed Completion Date: July 20, 2017

Actual Completion Date: July 20, 2017

File 1, "*RFC2017018261 Certification Package*", Conduct [redacted] bulk upload process-RFC2017018261, Page 2, illustrates that the subject matter expert responsible for conducting the bulk upload determined that three individuals that were being uploaded did not have proper

credentials to have the provisioned access. After identification, the subject matter expert proposed 2 definitive paths in order to revoke access.

Milestone # 3 Completion verified

Milestone 4: Remove access.

Proposed Completion Date: July 21, 2017

Actual Completion Date: July 21, 2017

File 1, "*RFC2017018261 Certification Package*", Remove access- RFC2017018261, Pages 1 through 4, shows an email from the subject matter expert with included screen grabs showing that the access had been removed due to the lack of required qualifications.

Milestone # 4 Completion verified

Milestone 5: Update the [redacted] Request for access SWI.

Proposed Completion Date: August 1, 2017

Actual Completion Date: August 1, 2017

File 1, "*RFC2017018261 Certification Package*", SWI-Template, Pages 1 through 9, show the updated template (8-1-2017) and the email communication that went out to affected staff per this change of process/ procedure per this milestone.

Milestone # 5 Completion verified

Milestone 6: Conduct a [redacted] Review of access.

Proposed Completion Date: August 30, 2017

Actual Completion Date: July 21, 2017

File 1, "*RFC2017018261 Certification Package*", Remove Access-RFC2017018261, Pages 1 through 4, shows the entity SME response to removing access with the users access that needs to be removed.

Milestone # 6 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-004-6

Requirement: CIP-004-6 R4.

Date Submitted: December 01, 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: April 01, 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 Processes

User access provisioning and revocation program - This program requires provisioning of users using a tool called [redacted] requires a valid NERC training, Personnel Risk Assessment (PRA), and request (Authorization Record) from the supervisor of the employee. This process supports CIP004 R4 Part 4.1

[redacted] (PAR) - In order to verify that electronic, physical, and BCSI access is appropriate [redacted] follows a [redacted] every quarter to determine accuracy of user access of all 'provisioned users in each application' relevant for NERC, SOX and PCI compliance. [redacted] process works by collecting list of roles/privileges (Data) for each user for each in scope applications, systems, and databases. This data is reviewed by the supervisors and the role owners to determine that the roles/privileges are correct and necessary. This process supports CIP004 R4 Part 4.3 and Part 4.4

[redacted] Process - In order to verify that active electronic access or unescorted physical access have authorization records, [redacted] performs another process, named the [redacted] process quarterly. [redacted] process is to compare authorization records from [redacted] with the roles/privileges granted to a user. [redacted] process works by obtaining the list of authorization records from [redacted] list of roles/privileges from [redacted] process, and comparing the two in

order to ensure that the individuals with active electronic access or unescorted physical access have authorization records. This process supports CIP004 R4 Part 4.2

Incident description
2017 Q3 process identified that users had access to share drive that holds the BCIS but the authorization record were not found in Further investigation showed that these as well, were marked for removal, and the supervisors were communicated to remove the access. The Supervisors for users had requested a revocation in based on the 2017 Q1 results. While system records indicates that the requests were completed and access was revoked, the he users still had access to the shared drives for which access was requested to be revoked. This implies that workflow was closed without the process confirming that the access to the shared drive was revoked.

In addition to the users from Q1, the results for 2017 Q3, indicated users as provisioned in different from what the results expected. These were treated as a regular outcome of the process that required follow-up and correction. The revocation process was immediately followed and corrected by the Supervisors.

*What is the problem?
2017 Qtr3 revealed that users identified to be removed in 2017Q1 process continued to have access to the shared drives (designated storage locations).
As ked as designed but authorization records for such access did not exist, this has been recorded as a violation of CIP-004- R4 P4.1 - "Process to authorize based on need, as determined by the Responsible Entity,except for CIP Exceptional Circumstances:
4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.".

*Root Cause of Possible Violation:
As per the & RCA performed on 10/31/2017, the root cause was identified to be Lack of validation of removal of access when identified during the process.

*How was the violation discovered?
On 09/29/2017, while concluding 2017 Q3 determined that 6 users discrepancies from Q1 process remained unresolved in Q3.

*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 a gap in the currently defined Process. The Supervisor closed the revocation of access ticket without checking for evidence of revocation. The process SWI needs to be updated and recirculated to the users involved with access management.

*Timeline:
09/29/2017 - 2017 Q3 completed.
09/29/2017 - Access management analyst reported users with access to shared drives and no valid record. showed access revoked. These users had been repeatedly been an issue since Q1.
10/31/2017 - RCA was performed to understand the sequence of events in the process and it was identified that there was a gap in the process. The process did not require evidence of access revocation prior to closing an tickets.

Self Report

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Corrective Actions:
Access for these [redacted] users have been revoked since identification of this issue.

Mitigating and Preventive measures:
Update the [redacted] process to include validation of the removal of access.

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
Potential impact of users having access to these could be severe as the share drive includes the BCSI relevant to process, procedures, and programs.

Actual Impact
The users with access to shared drives that needed to be revoked, were [redacted] personal who had background clearance and were trained in NERC CIP standards prior to being granted access via [redacted] The revocation process did not get concluded for these users since the Supervisor closed the [redacted] ticket to revoke access without evidence.

Risk Assessment of Impact to BPS: The risk was measured as low because all of the users with access to the share drive had a valid PRA and had a valid training record.

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
RFC2017018760	CIP-004-6 R4.	

Mitigation Plan Submitted On: December 14, 2017

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: January 10, 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		
RFC2017018760	04/01/2017	CIP-004-6 R4.
Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.		

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

Brief Description: (What happened?)
Current Processes
User access provisioning and revocation program - This program requires provisioning of users using a tool called [redacted] requires a valid NERC training, Personnel Risk Assessment (PRA), and request (Authorization Record) from the supervisor of the employee. This process supports CIP004 R4 Part 4.1

[redacted] - In order to verify that electronic, physical, and BCSI access is appropriate [redacted] follows a [redacted] every quarter to determine accuracy of user access of all 'provisioned users in each application' relevant for NERC, [redacted] compliance. [redacted] process works by collecting list of roles/privileges (Data) for each user for each in scope applications, systems, and databases. This data is reviewed by the supervisors and the role owners to determine that the roles/privileges are correct and necessary. This process supports CIP004 R4 Part 4.3 and Part 4.4

[redacted] Process - In order to verify that active electronic access or unescorted physical access have authorization records, [redacted] performs another process, named the [redacted] process quarterly. [redacted] process is to compare authorization records from [redacted] with the roles/privileges granted to a user. [redacted] process works by obtaining the list of authorization records from [redacted] list of roles/privileges from [redacted] process, and comparing the two in order to ensure that the individuals with active electronic access or unescorted physical access have authorization records. This process supports CIP004 R4 Part 4.2

Incident description
2017 Q3 [redacted] identified that [redacted] users had access to share drive that holds the BCIS but the authorization record were not found in [redacted] Further investigation showed that these [redacted] users were identified in 2017 Q1 [redacted] as well, were marked for removal, and the supervisors were communicated to remove the access. The Supervisors for [redacted] users had requested a revocation in [redacted] based on the 2017 Q1 results. While [redacted] system records indicates that the requests were completed and access was revoked, the [redacted] for Q3 indicates that the [redacted] users still had access to the shared drives for which access was requested to be revoked. This implies that [redacted] workflow was closed without the [redacted] confirming that the access to the shared drive was revoked.

In addition to the [redacted] users from Q1, the [redacted] process results for 2017 Q3, indicated [redacted] users as provisioned in [redacted] different from what the [redacted] results expected. These were treated as a regular outcome of the [redacted] process that required follow-up and correction. The revocation process was immediately followed and corrected by the Supervisors.

Cause: (what caused the violation?)

2017 Qtr3 [redacted] revealed that users identified to be removed in 2017Q1 [redacted] continued to have access to the shared drives (designated storage locations).
As [redacted] worked as designed but authorization records for such access did not exist, this has been recorded as a violation of CIP-004- R4 P4.1

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

As per the [redacted] & RCA performed 10/31/2017, the root cause was identified to be Lack of validation of removal of access when identified during the [redacted] process.

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

On 09/29/2017, while concluding 2017 Q3 [redacted] determined that [redacted]users discrepancies from Q1 [redacted] process remained unresolved in Q3.

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 - Access for these [redacted] users to be revoked for the shared drives to correct current access requirements

Access for these [redacted] users have been revoked since identification of this issue. The Supervisors were contacted and requested to remove access (outside of [redacted] and monitor that the action was taken, including emailing an evidence to the account management team for each discrepancy resolved.

Milestone 2 - Update the [redacted] process to include validation of the removal of access
Review and update process [redacted] process for Access removal request. [redacted] process will include validation of removal actions. The team that executes quarterly [redacted] process is team of [redacted] members. This team has incorporated the validation of removal in current practice (in order to complete Q4 [redacted] process). However, it will be formalized by end of December.

Milestone 3 - Communicate the [redacted] process to include validation of the removal of access
Communicate the update to the [redacted] process to the set of Supervisors responsible for managing the access authorizations.

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 10, 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
1. Access for these [redacted] users to be revoked for the shared drives	Contact the Supervisors of all [redacted] users to revoke access to the shared drive per the [redacted] results.	11/29/2017	11/29/2017		No
2. Update the [redacted] process to include validation of the removal of access	Review and update process [redacted] process for Access removal request. [redacted] process will include validation of removal actions. The team that executes quarterly [redacted] process is team of [redacted] members. This team	01/10/2018			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
	has incorporated the validation of removal in current practice (in order to complete Q4 [redacted] process). However, it will be formalized by end of December.				
3. Communicate the updated [redacted] process	Communicate the update to the team responsible for managing the access authorizations.	01/10/2018			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.

[redacted] has not identified any risk to the BES. The risk was measured as low because all of the users with access to the share drive had a valid HR clearance as [redacted] employees and had a valid NERC CIP training record. Validation of removal has been incorporate in current practice and will be tested while performing the [redacted] for Q4.

Potential impact of users having access to these could be severe as the share drive includes the BCSI relevant to process, procedures, and programs.

These include revocation of access for 6 users whose roles have undergone a change and hence access is no longer needed to the shared drive, and an update of the [redacted] process to ensure revocation was successfully performed before [redacted] tickets are closed in the future.

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

[redacted] will prevent such occurrences in the future by updating the gap in the [redacted] process itself. Currently, an [redacted] ticket can be closed by the Supervisor without reviewing access revocation evidence. In the updated process, an evidence would need to be provided as a backup to close an [redacted] ticket. This would prevent an occurrence whereby [redacted] shows no access, while the user continued to have access in the shared drive.

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): RFC2017018760
Mitigated Standard Requirement(s): CIP-004-6 R4.
Scheduled Completion as per Accepted Mitigation Plan: January 10, 2018
Date Mitigation Plan completed: January 10, 2018
RF Notified of Completion on Date: January 17, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017018760 Certification Package.zip	File "RFC2017018760 Certification Package" contains the coversheet for the package. This zip file also contains the supporting data for each milestone.	706,130

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 RFC2017018760

[redacted]

Standard/Requirement: CIP-004-6 R4

NERC Mitigation Plan ID: RFCMIT013443

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 12/01/17	12/14/17	01/04/18	01/26/18	01/17/18	01/10/18

Description of Issue

The user access provisioning and revocation program requires provisioning of users using a tool called [redacted] requires a valid NERC training, Personnel Risk Assessment (PRA), and request (Authorization Record) from the supervisor of the employee.

In order to verify that active electronic access or unescorted physical access have authorization records, [redacted] performs a [redacted] process quarterly to compare authorization records from [redacted] with the roles/privileges granted to a user.

The 2017 third quarter [redacted] process identified that [redacted] users had access to a shared drive that holds the BCIS, but the authorization records were not found in [redacted] Further investigation showed that these [redacted] users were identified in 2017 first quarter [redacted] as well, were marked for removal, and the supervisors were told to remove the access. The Supervisors for [redacted] users had requested a revocation in [redacted] based on the 2017 first quarter results. While [redacted] system records indicate that the requests were completed and access was revoked, the [redacted] for the third quarter indicates that the [redacted] users still had access to the shared drives for which access was requested to be revoked. This implies that [redacted] workflow was closed without the [redacted] process confirming that the access to the shared drive was revoked.

The root cause was identified to bel of validation of removal of access when identified during the [redacted] process.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017018760 Certification Package	CIP-004-6 R4
File 2	RFC2017018760 Milestone 3 Submit	CIP-004-6 R4
File 3	RFC2017018760 Milestone 2 Additional Evidence	CIP-004-6 R4

Verification of Mitigation Plan Completion

Milestone 1: Access for these [redacted] users to be revoked for the hard drives.

Proposed Completion Date: November 29, 2017

Actual Completion Date: November 29, 2017

File 1, "*RFC2017018760 Certification Package*", Milestone 1- Submit, Page 2, in the highlighted areas shows the [redacted] users removed from active directory as specified in milestone 1.

Milestone # 1 Completion verified.

Milestone 2: Update the [redacted] process to include validation of the removal of access.

Proposed Completion Date: January 10, 2018

Actual Completion Date: January 22, 2017

File 3, "*RFC2017018760 Milestone 2 Additional Evidence*", NERC Remediation [redacted] process, Pages 1 and 2, show the [redacted] process that includes a validation step.

Milestone # 2 Completion verified.

Milestone 3: Communicate the updated [redacted] process.

Proposed Completion Date: January 10, 2018

Actual Completion Date: January 18, 2018

File 1, "*RFC2017018760 Certification Package*", Milestone 3- Submit, Page 2 shows an email with an attached process which was sent to 6 email addresses.

File 2, "*RFC2017018760 Milestone 3 Submit*", Page 2, shows the email that was sent in regards to the updated process.

Milestone # 3 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: March 12, 2018

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Attachment 5

Record documents for the violation of CIP-004-6 R5

5.a The Entity's Self-Report (RFC2017017152) submitted [redacted];
5.b The Entity's Self-Report (RFC2017017152) submitted [redacted];
5.c The Entity's Mitigation Plan designated as RFCMIT012807-1 submitted [redacted];
5.d The Entity's Certification of Mitigation Plan Completion dated [redacted];
5.e ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted]

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-004-6

Requirement: CIP-004-6 R5.

Date Submitted: February 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: December 12, 2016 **Changed to December 9, 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 December 8, 2016, one contract [redacted] working at [redacted] resigned from [redacted] (a contract security company for [redacted] This action caused the [redacted] site supervisor to de-activate the employees' ID badge. On January 10, 2017, [redacted] gathered data for the 1st quarter [redacted] The [redacted] employee compares the [redacted] and the [redacted] reports and notices that one contract employee [redacted] is activate in the [redacted] system in the [redacted] system (Cyber Access for the PACS system), but their badge is de-activated in the PACS system [redacted] In other words, it became apparent that the employee [redacted] retained cyber access to the PACS system for more than 24 hours after separating from employment, which means the contract employee [redacted] had remote login access capabilities. The contract employee worked at [redacted]. However, since the employee had remote login access capabilities to the PACS associated [redacted] BES Cyber Systems for more than 24 hours after termination this is the violation.

Root Cause of Possible Violation: Contract employee [redacted] separated employment and his leader did not follow the [redacted] termination process to remove employees' access which rarely happens at [redacted]

How was the violation discovered? On January 10, 2017, [redacted]

Self Report

employee was gathering data for the 1st quarter [redacted] ([redacted] employee compared the [redacted] and the [redacted] reports and noticed that one contact employee [redacted] was activate in the [redacted] system and in the [redacted] system, but their badge (physical access) was de-activated in the PACS system [redacted]

Timeline:
12/08/2017 - Contract employee [redacted] from [redacted] resigned from [redacted] (contract security company for [redacted]
12/08/2016 - [redacted] site supervisor de-activated contract employees' [redacted] ID badge access. However, access to [redacted] remote login, and authorization for Physical and Cyber Access was not disabled within the 24 hour allotted time causing the violation.
01/10/2017 - While [redacted] employee was gathering information for our 1st quarter [redacted] ([redacted] and compared this information to the [redacted] ([redacted] and noticed one contract employee [redacted] was activate in the [redacted] system and in the [redacted] system, but their badge was de-activated in our PACS system [redacted]
01/10/2017 - [redacted] employee initiated and processed the revocation of one contract employees' [redacted] physical access, remote login access, and [redacted] user account.
01/11/2017 & 01/25/2017 - [redacted] leader went through all [redacted] direct reports on two occasions to ensure every employee is still active and has appropriate access.
01/11/2017 - [redacted] leader held a two-hour face to face meeting with entire group to discuss the proper [redacted] process for removal of access. [redacted] leader also re-disseminated the process map via email to advise the entire group of the correct [redacted] process.
01/31/2017 - [redacted] leader verified that employee [redacted] had remote access during the time of the PV, but did not log in remotely at any time during the violation period.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Description of Mitigating Activities: 1. The execution of Quarterly [redacted] acted as a control to detect potential CIP004 violations. 2. Physical ID badge was disabled

Description of Preventative Measures: 1. [redacted] went through all [redacted] direct reports on two occasions (January 11, 2017 and January 25, 2017) to ensure every employee is still active and had appropriate access. 2. On January 11, 2017, [redacted] held a two-hour face to face meeting with entire group to discuss the proper [redacted] process for removal of access 3. On January 11, 2017, [redacted] re-disseminated the process map via email to advise the entire group of the correct [redacted] process

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 is determined to be minimal because on January 31, 2017, [redacted] employee verified that during the violation time period 12/8/2016 - 01/10/2017 the employee had remote access but did not log in remotely.

[redacted] has not experienced any negative impact to its Bulk

Self Report

Risk Assessment of Impact to BPS: 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

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-004-6

Requirement: CIP-004-6 R5.

Date Submitted: March 01, 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: January 08, 2017

End/Expected End Date: January 30, 2017

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: [redacted] is a server that enforces dual authentication. This server is classified as an EACMS for [redacted] assets. A shared account [redacted] is used to manage [redacted] server. The password for this account is known to only those who are listed in a document that is maintained by respective business units. On January 26 during an internal QA review of data, including list of users with access to shared accounts, for CIP004 R5.5, it was discovered that an employee of [redacted] ([redacted] voluntarily left the company and who knew password for '[redacted] account. Further review shows that the password for the account was not changed within 30 days of the termination, violating NERC CIP004 R5.5. We further verified that all other Physical and Cyber access for this employee was removed promptly. The password for the shared account was changed immediately after finding the violation.

*Root Cause of Possible Violation:
[redacted] has a system access control procedure and [redacted] policy program that states passwords must be changed for each shared account to which the employee has authorized access within 30 days of the termination action. However, the procedure was not followed due to a lack of knowledge transfer. Yet, the password was changed after the issue was discovered.
A new SME took over the responsibilities of managing [redacted] servers. Lack of roles transitioning failure within [redacted] was determined to be the cause of the violation.

Self Report

*How was the violation discovered?
Violation was discovered during an internal QA review of data for CIP004 R5.5.

*Timeline:
1. December 9, 2017 - the employee left the company.
2. December 9, 2017 - Interactive remote access and unescorted physical access was removed.
3. January 26, 2017 - QA review discovered this issue.
4. January 30, 2017 - the password was changed.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Mitigating:
Interactive Remote access and unescorted physical access was removed promptly (following procedure and requirement CIP004 Part 5.1)
Password of [redacted] account was changed after discovering the violation.

Preventative Measures:
• [redacted] will update the System Access Control Procedures shared account inventory to reflect the current shared account inventory.
• A procedure will be developed by [redacted] to include a check list for transitioning SMEs between the roles.
• Will perform quality check across all BCAs to see if there are other similar occurrences (Extent of condition)

Date Mitigating Activities Completed: March 08, 2017

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 as Interactive remote access and unescorted physical access was removed the same day the employee left the company. The Actual Impact to the BES is none as [redacted] has not experienced a situation where the BES was negatively impacted as a result of delayed shared account password change.

Risk Assessment of Impact to BPS: [redacted] identifies that potential impact to the BES is low due to the individual who got terminated did not have the password of the shared drive.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes

Self Report

No Documents

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
RFC2017017152	CIP-004-6 R5.	

Mitigation Plan Submitted On: April 12, 2017

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: May 23, 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		
RFC2017017152	12/12/2016	CIP-004-6 R5.
Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.		

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

Incident 1:

On December 8, 2016, one contract employee working at [redacted] resigned from [redacted] a contract security company for [redacted] This action caused the [redacted] site supervisor to de-activate the employees' ID badge. On January 10, 2017, [redacted] gathered data for the 1st quarter [redacted] The [redacted] employee compares the [redacted] and the [redacted] reports and notices that one contract employee is activated in the [redacted] system in the [redacted] system (Cyber Access for the PACS system), but their badge is de-activated in the PACS system [redacted] It was apparent that the employee retained cyber access to the PACS system for more than 24 hours after separating from employment, so the contract employee had remote login access capabilities. The contract employee worked at [redacted]. However, since the employee had remote login access capabilities to the PACS associated with the [redacted] BES Cyber Systems for more than 24 hours after termination, this is the violation.

Incident 2:

[redacted] is a server that enforces dual authentication. This server is classified as an EACMS for [redacted] assets. A shared account '[redacted] is used to manage [redacted] server. The password for this account is known to only those who are listed in a document that is maintained by respective business units. On January 26 during an internal QA review of data that included the list of users with access to shared accounts for CIP004 R5.5, it was discovered that an employee of [redacted] voluntarily left the company with knowledge of the password for '[redacted] account. Further review shows that the password for the account was not changed within 30 days of the termination, violating NERC CIP004 R5.5. We further verified that all other Physical and Cyber access for this employee was removed promptly. The password for the shared account was changed immediately after finding the violation.

Cause of Possible Violation:

Incident 1: Contract employee separated employment and his leader did not follow the [redacted] termination process to remove employees' access. Termination of personnel with NERC CIP authorized access rarely occurs at [redacted] a [redacted] BES asset.

Incident 2: [redacted] has a system access control procedure and [redacted] policy program that states passwords must be changed for each shared account to which the employee has authorized access within 30 days of the termination action. However, the procedure was not followed due to a lack of knowledge transfer for new responsible SME. Yet, the password was changed after the issue was discovered.
A new SME took over the responsibilities of managing [redacted] servers. Lack of roles transitioning failure within [redacted] was determined to be the cause of the violation.

Timeline:

Incident 1:

12/08/2017 - Contract employee from [redacted] resigned from [redacted] (contract security

company for [redacted]
12/08/2016 - [redacted] site supervisor de-activated contract employees' ID badge access. However, access to [redacted] remote login, and authorization for Physical and Cyber Access was not disabled within the 24 hour allotted time causing the violation. The employee retained cyber access to the PACS system for more than 24 hours after separating from employment, which means the contract employee had remote login access capabilities.
01/10/2017 - While [redacted] employee was gathering information for our 1st quarter [redacted] ([redacted] and compared this information to the [redacted] and noticed one contract employee was active in the [redacted] system and in the [redacted] system, but their badge was de-activated in our PACS system ([redacted]
01/10/2017 - [redacted] employee initiated and processed the revocation of one contract employees' physical access, remote login access, and [redacted] user account.
01/11/2017 & 01/25/2017 - [redacted] leader went through all [redacted] direct reports on two occasions to ensure every employee is still active and has appropriate access.
01/11/2017 - [redacted] leader held a two-hour face to face meeting with entire group to discuss the proper [redacted] process for removal of access. [redacted] leader also re-disseminated the process map via email to advise the entire group of the correct [redacted] process.
01/31/2017 - [redacted] leader verified that employee had remote access during the time of the PV, but did not log in remotely at any time during the violation period.
Incident 2:
12/9/2016 - the employee left the company.
12/9/2016 - Interactive remote access and unescorted physical access was removed.
1/26/2017 - QA review discovered this issue.
1/30/2017 - the password was changed

What is the violation?

Incident 1: The contract employee worked at [redacted] [redacted]. However, since the employee had remote login access capabilities to the PACS associated [redacted] BES Cyber Systems for more than 24 hours after termination this is the violation.

Incident 2: A shared account password was not changed within 30 days of the termination, violating NERC CIP004 R5.5.

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

How was the violation discovered?

Incident 1: On January 10, 2017, [redacted] employee was gathering data for the 1st quarter [redacted] ([redacted] [redacted] employee compared the [redacted] and the [redacted] ([redacted] reports and noticed that one contract employee was activated in the [redacted] system and in the [redacted] system, but their badge (physical access) was de-activated in the PACS system ([redacted]

Incident 2: Violation was discovered during an internal QA review of data for CIP004 R5.5.

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:

Milestones below show the detailed actions [redacted] is undertaking to mitigate the violation.

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: May 23, 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
Instance 1- Hold [redacted] Security / Vendor Meeting	Go through all leader's [redacted] employees managed to determine if all employees still working on [redacted] account	01/11/2017	01/11/2017		No
Instance 1- Revoke access	Revoke NERC Access	01/11/2017	01/10/2017		No
Instance 1- Training	Retrain leaders on non-EE deactivation process	01/11/2017	01/11/2017		No
Instance 2- Milestone 1	[redacted] will update the System Access Control Procedures shared account inventory to reflect the current shared account inventory.	03/08/2017	03/16/2017		No
Instance 2- Milestone 2	A procedure will be developed by [redacted] to include a check list for transitioning SMEs between the roles.	03/08/2017	03/23/2017		No
Instance 2- Milestone 3	Will perform quality check across all BCAs to see if there are other similar occurrences (Extent	05/23/2017			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
	of condition)				

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 risk to the BES is determined to be minimum because both the terminations were volunteer separations. Review of logs shows no activity from respective IDs after the separation date.

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 by updating the System Access Control Procedures shared account inventory to reflect the current shared account inventory and the procedure will be developed by [redacted] to include a check list for transitioning SMEs between roles.

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: April 11, 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): RFC2017017152
Mitigated Standard Requirement(s): CIP-004-6 R5.
Scheduled Completion as per Accepted Mitigation Plan: May 23, 2017
Date Mitigation Plan completed: May 18, 2017
RF Notified of Completion on Date: May 30, 2017
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017152 Certification Package - Submit.zip	A ZIP file "RFC2017017152 Certification Package.zip" contains the following: RFC2017017152 Cover Page - Submit.pdf - Cover page for overall package. This violation was combination of two different violations (Instance 1 and Instance 2). Instance 1-Milestone 1 - Submit.pdf - Contains evidence to support completion of milestone 1 for instance 1. Instance 1-Milestone 2 - Submit.pdf - Contains evidence to support completion of milestone 2 for instance 1. Instance 1-Milestone 3 - Submit.pdf - Contains evidence to support completion of milestone 3 for instance 1. Instance 2-Milestone 1 - Submit.pdf - Contains evidence to support completion of milestone 1 for instance 2. Instance 2-Milestone 2 - Submit.pdf - Contains evidence to support completion of milestone 2 for instance 2. Instance 2-Milestone 3 - Submit.zip - Contains	4,237,443

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017152 Certification Package - Submit.zip	evidence to support completion of milestone 3 for instance 2.	4,237,443
Entity	Instance 2-Milestone 3 - Submit-NEW.zip	File Instance 2-Milestone 3 - Submit-NEW.zip contains Instance 2-Milestone 3 - Submit. PDF. This has to be zipped and uploaded separately as it was greater than 50MB file.	45,698,735

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 RFC2017017152

[redacted]

Standard/Requirement: CIP-004-6 R5

NERC Mitigation Plan ID: RFCMIT012807-1

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 02/24/17 03/01/17	04/12/17	04/12/17		05/30/17	05/18/17

Description of Issue

Incident 1:

On December 8, 2016, a contract employee working at [redacted] resigned from [redacted] a contract security company for [redacted] This action caused the [redacted] site supervisor to de-activate the employees' ID badge. On January 10, 2017, [redacted] gathered data for the 1st quarter via a [redacted] ([redacted] The [redacted] employee compares the [redacted] and the [redacted] ([redacted] reports and notices that one contract employee is activated in the [redacted] system in the [redacted] system (Cyber Access for the PACS system), but their badge is deactivated in the PACS system ([redacted] It was apparent that the employee retained cyber access to the PACS system for more than 24 hours after separating from employment, therefore, the contract employee had remote login access capabilities. The contract employee worked at [redacted] [redacted] [redacted]. However, since the employee had remote login access capabilities to the PACS associated with [redacted] BES Cyber Systems for more than 24 hours after termination, this is a violation.

Incident 2:

[redacted] is a server that enforces dual authentication. This server is classified as an EACMS for [redacted] assets. A shared account '[redacted] is used to manage the [redacted] server. The password for this account is known to only those who are listed in a document that is maintained by respective business units. On January 26, during an internal QA review of data that included the list of users with access to shared accounts for CIP004 R5.5, it was discovered that an employee of [redacted] ([redacted] voluntarily left the company with knowledge of the password for '[redacted] account. Additional review shows that the password for the account was not changed within 30 days of the termination, violating NERC CIP004 R5.5. We further verified that all other Physical and Cyber access for this employee was removed promptly. The password for the shared account was changed immediately after finding the violation.

Cause of Possible Violation:

Incident 1: Contract employee separated employment and his leader did not follow the [redacted] termination process to remove employees' access. Termination of personnel with NERC CIP authorized access rarely occurs at [redacted] a [redacted] BES asset.

Incident 2: [redacted] has a system access control procedure and [redacted] policy program that states passwords must be changed for each shared account to which the employee has authorized access within 30 days of the termination action. However, the procedure was not followed due to a lack of knowledge transfer for new responsible SME. Yet, the password was changed after the issue was discovered.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017017152 Certification Package-Submit	CIP-004-6 R5
File 2	Instance 2 Milestone 3- Submit-NEW	CIP-004-6 R5

Verification of Mitigation Plan Completion

Milestone 1: Instance 1- Hold [redacted] Security/Vendor Meeting.

File 1, "*RFC2017017152 Certification Package- Submit (ZIP File Folder)",* Instance 1 – Milestone 1- Submit (File Name), Pages 2 through 5, provide evidence as to the occurrence of a [redacted] Security and Vendor meeting to discuss the PNC of CIP-004-6 R5. In addition, two agendas and attendance rosters were also provided (Page 2 and Page 5).

Milestone #1 Completion Verified.

Milestone 2: Instance 1- Revoke access.

File 1, "*RFC2017017152 Certification Package- Submit (ZIP File Folder)"*, Instance 1 –Milestone 2- Submit(File Name), Pages 2 through 7, show how [redacted] CIP environment is labeled in order to provide evidence and explanation into the requests to revoke access according to Milestone 2 and to demonstrate that no access/access events occurred during the time of this potential noncompliance. Pages 8 through 11 provide tickets for access revocation as required by Milestone 2.

Milestone #2 Completion Verified.

Milestone 3: Instance 1- Training.

File 1, "*RFC2017017152 Certification Package- Submit (ZIP File Folder)"*, Instance 1 –Milestone 3 –Submit (File Name), Page 2 of 14, provides an email with attachments that was delivered to affected employees in order to reinforce the revocation process. Page 3 of 14, shows the process workflow for the revocation of access while Pages 5 through 12, walk a user through the steps of how to formally request and/or remove access via their enterprise business system.

Milestone # 3 Completion Verified.

Milestone 4: Instance 2- Milestone 1

File 1, "*RFC2017017152 Certification Package- Submit (ZIP File Folder)"*, Instance 2 –Milestone 1 –Submit (File Name), Pages 7 and 8, illustrate the update to the System Access Control Procedures shared account inventory as specified by this milestone. Page 12 shows the revision history of this update from January 30, 2017, which specifies these changes and their location within the document.

Milestone #4 Completion Verified.

Milestone 5: Instance 2- Milestone 2

File 1, "*RFC2017017152 Certification Package- Submit (ZIP File Folder)",* Instance 2 –Milestone 2 –Submit (File Name), Pages 2 through 5, show the checklist for transitioning SMEs required by this milestone.

Milestone # 5 Completion Verified.

Milestone 6: Instance 2 -Milestone 3.

File 2, "*Instance 2- Milestone 3- Submit-New (Zip File Folder)",* Instance 2- Milestone 3 – Submit –New (File Name), Pages 15 through 265, show the extent of condition analysis performed in regard to access revocation when employees have changed roles, or left the company.

Milestone # 6 Completion Verified.

The Mitigation Plan is hereby verified complete.

Date: June 22, 2017

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Attachment 6

Record documents for the violation of CIP-005-5 R2

6.a The Entity's Self-Report (RFC2018019570);
6.b The Entity's Mitigation Plan designated as RFCMIT013868 submitted [redacted];
6.c The Entity's Certification of Mitigation Plan Completion dated [redacted];
6.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted]

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-005-5

Requirement: CIP-005-5 R2.

Date Submitted: April 11, 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: November 13, 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: Current Process:

[redacted]

Incident description:

[redacted]

Methodology summary:

Self Report

[redacted]

Self Report

[redacted]

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: [redacted]

Self Report

[redacted]

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: [redacted]

[redacted]

Risk Assessment of Impact to BPS: [redacted]

Additional Entity Comments: [redacted]

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

[redacted]

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
[redacted]	[redacted]	

Mitigation Plan Submitted On: June 13, 2018

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: August 15, 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		
[redacted]	[redacted]	[redacted]
Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in [redacted]		

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

Current Process:

[redacted]

Incident description:

[redacted]

Methodology summary:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[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:

[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: August 15, 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
[redacted]	[redacted]	11/15/2017	11/15/2017		No
[redacted]	[redacted]	12/04/2017	12/04/2017		No
[redacted]	[redacted]	12/05/2017	12/05/2017		No
[redacted]	[redacted]	12/05/2017	12/05/2017		No
[redacted]	[redacted]	12/05/2017	12/05/2017		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]				
[redacted]	[redacted]	12/06/2017	12/06/2017		No
[redacted]	[redacted]	01/30/2018	01/30/2018		No
[redacted]	[redacted]	04/16/2018	04/16/2018		No
[redacted]	[redacted]	06/25/2018			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]	[redacted]	06/28/2018			No
[redacted]	[redacted]	07/03/2018			No
[redacted]	[redacted]	07/30/2018			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
	[redacted]				
[redacted]	[redacted]	08/06/2018			No
[redacted]	[redacted]	[redacted]			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]				
[redacted]	[redacted]	08/15/2018			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.

[redacted]

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

[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

[redacted]

[redacted]

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 13, 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): [redacted]
Mitigated Standard Requirement(s): [redacted]
Scheduled Completion as per Accepted Mitigation Plan: August 15, 2018
Date Mitigation Plan completed: August 15, 2018
RF Notified of Completion on Date: August 15, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[redacted] Certification Package.zip	Zip file '[redacted] Certification Package.zip" contains evidence supporting completion of each milestone. There is one PDF file for each milestone. An excel sheet "Milestone 11 - Completion Report - Required Read" is in support to "Milestone 1 - Submit.PDF"	21,751,684

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 [redacted]

[redacted]

Standard/Requirement: [redacted]

NERC Mitigation Plan ID: [redacted]

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Documents	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Reports 04/11/18	06/13/18	07/12/18	10/05/18	08/15/18	08/03/18

Description of Issue

Mitigation Plan Task RFC2018019567 et al

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	[redacted] Certification Package	[redacted]
File 2	[redacted] Certification Package Updated	[redacted]

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
		[redacted]
File 3	[redacted]	[redacted]

Verification of Mitigation Plan Completion

Milestone 1: [redacted].

Proposed Completion Date: November 15, 2017

Actual Completion Date: November 15, 2017

File 2, '[redacted] *Certification Package Updated*," Milestone 1 – Submit at Pages 2 through 12, shows: [redacted]

Milestone # 1 Completion verified.

Milestone 2: [redacted].

Proposed Completion Date: December 4, 2017

Actual Completion Date: December 15, 2017

File 2, '[redacted] *Certification Package Updated*," Milestone 2 – Submit at Pages 2 and 3, contains a signed attestation, which includes a statement explaining that [redacted]

Milestone # 2 Completion verified.

Milestone 3: Correct vulnerable configuration on [redacted].

Proposed Completion Date: December 5, 2017

Actual Completion Date: May 2, 2018

File 2, '[redacted] *Certification Package Updated*," Milestone 3 – Submit at Pages 2 through 11, shows that the entity disabled [redacted].

Milestone # 3 Completion verified.

Milestone 4: [redacted]

Proposed Completion Date: December 5, 2017

Actual Completion Date: December 15, 2017

File 2, '[redacted] *Certification Package Updated*", Milestone 4 – Submit at Pages 2 and 3, contains a signed attestation, which includes a statement explaining that [redacted].

Milestone # 4 Completion verified.

Milestone 5: [redacted].

Proposed Completion Date: December 5, 2017

Actual Completion Date: December 5, 2017

File 2, '[redacted] *Certification Package Updated*," Milestone 5 – Submit at Pages 2 through 445, shows that the entity [redacted].

Milestone # 5 Completion verified.

Milestone 6: [redacted]

Proposed Completion Date: December 6, 2017

Actual Completion Date: November 20, 2017

File 2, "[redacted] *Certification Package Updated*," Milestone 6 – Submit at Pages 2 and 3, contains a signed attestation, which includes a statement explaining that [redacted]

Milestone # 6 Completion verified.

Milestone 7: [redacted]

Proposed Completion Date: January 30, 2018

Actual Completion Date: January 30, 2018

File 2, [redacted] *Certification Package Updated*," Milestone 7 – Submit at Pages 2 through 12, shows that the entity [redacted]

Milestone # 7 Completion verified.

Milestone 8: [redacted].

Proposed Completion Date: June 25, 2018

Actual Completion Date: June 25, 2018

File 2, "[redacted] *Certification Package Updated*," Milestone 9 – Submit at Pages 2 through 8, contains: (a) pre- and post-[redacted] and [redacted]

Milestone # 8 Completion verified.

Milestone 9: [redacted]

Proposed Completion Date: June 28, 2018

Actual Completion Date: June 22, 2018

File 2, '[redacted] *Certification Package Updated*," Milestone 10 – Submit at Pages 2 through 11, shows the updated program, which includes [redacted] The same file at Pages 12 and 13 shows the email sent out regarding the updates along with contact information if staff had questions or concerns.

Milestone # 9 Completion verified.

Milestone 10: Create a process for [redacted].

Proposed Completion Date: July 3, 2018

Actual Completion Date: August 3, 2018

File 2, '[redacted] *Certification Package Updated*," Milestone 11 – Submit at Pages 2 through 10, contains a process diagram, a standard work instruction, and emails communicating the diagram and standard work instruction. File 2, [redacted] *Certification Package Updated*," Milestone 10 – Submit at Pages 2 through 14, shows an updated program, which includes [redacted]

Milestone # 10 Completion verified.

Milestone 11: [redacted]

Proposed Completion Date: July 30, 2018

Actual Completion Date: July 5, 2018

File 2, '[redacted] *Certification Package Updated*," Milestone 11 – Submit at Pages 2 through 15, shows the standard work instruction that was updated to reflect revocation of access after 120 days of consecutive non-use.

Milestone # 11 Completion verified.

Milestone 12: Perform risk assessment on [redacted].

Proposed Completion Date: August 6, 2018

Actual Completion Date: July 20, 218

File 2, "[redacted] *Certification Package Updated*," Milestone 13 – Submit at Pages 2 through 5, contains documents evidencing the entity's risk assessment of [redacted]

Milestone # 12 Completion verified.

Milestone 13: Deploy [redacted]

Proposed Completion Date: August 13, 2018

Actual Completion Date: July 23, 2018

File 2, "[redacted] *Certification Package Updated*," Milestone 14 – Submit at Pages 2 through 37, shows the approved change order requests for the [redacted]

Milestone # 13 Completion verified.

Milestone 14: Communicate updated and newly created process(es).

Completion Date: August 15, 2018

Actual Completion Date: August 3, 2018

File 2, "[redacted] *Certification Package Updated*", Milestone 7 – Submit, Milestone 10 – Submit, Milestone 11 – Submit, and Milestone 12 – Completion Report, contain the relevant communications and/or records of communications.

Milestone # 14 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: February 7, 2019

Anthony Jablonski
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Attachment 7

Record documents for the violations of CIP-006-6 R1

7.a The Entity's Self-Report (RFC2017017304);
7.b The Entity's Mitigation Plan designated as RFCMIT012854 submitted [redacted];
7.c The Entity's Certification of Mitigation Plan Completion dated [redacted];
7.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted];
7.e The Entity's Self-Report (RFC2017017547);
7.f The Entity's Mitigation Plan designated as RFCMIT012890 submitted [redacted];
7.g The Entity's Certification of Mitigation Plan Completion dated [redacted];
7.h ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted];
7.i The Entity's Self-Report (RFC2017018166);
7.j The Entity's Mitigation Plan designated as RFCMIT013214 submitted [redacted];
7.k The Entity's Certification of Mitigation Plan Completion dated [redacted];
7.l ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted];
7.m The Entity's Self-Report (RFC2017018857);
7.n The Entity's Mitigation Plan designated as RFCMIT013482 submitted [redacted];
7.o The Entity's Certification of Mitigation Plan Completion dated [redacted];
7.p ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted]

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-006-6

Requirement: CIP-006-6 R1.

Date Submitted: March 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: August 10, 2016 **Changed to January 20, 2017**

End/Expected End Date:

Reliability Functions: [redacted]

Is Possible Violation still occurring?: No

Number of Instances: 5

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: NOTE: The first two instances were previously reported on September 21, 2016 (NERC Violation ID: [redacted]). They are included in this self-report only to show the trend of door hardware failures occurring at [redacted]

Instance 1 (Reported in [redacted]): On 08/10/2016 at 8:52 am a [redacted] Physical Access Control System (PACS) invalid attempt alarm was received by the [redacted] for Physical Security Perimeter (PSP) door [redacted] Investigation of the alarm revealed an employee without valid authorized unescorted access swiped his badge at the PSP door then proceeded to pull the handle of the door and the door opened.

Instance 2 (Reported in [redacted]): On 08/18/2016 at 5:22 pm a forced door alarm was received by the [redacted] for PSP door [redacted] Investigation of the alarm revealed that a contractor working outside of the PSP door was able to pull the door open without valid authorized access (swiping the badge).

Instance 3: On 01/20/2017 at 12:50:48 and again at 12:51:37 an employee without valid authorized unescorted access swiped her badge at [redacted] PSP door [redacted] Both attempts generated an invalid attempt alarm followed by a forced door alarm monitored by the [redacted] The

employee was able to access PSP door [redacted] on the second attempt due to an intermittent door equipment failure. [redacted]

Instance 4: On 01/26/17 the [redacted] received a door ajar alarm on PSP door [redacted] PSP door [redacted] During investigation of the alarm by a security officer, the door was pushed shut but the door ajar alarm would not clear. [redacted] Upon further investigation it was discovered that the [redacted] Upon completion of cooling, [redacted] The [redacted] was reviewed to verify that security was notified and alternate measures were put in place while the doors were propped open per [redacted] procedures.

Instance 5: On 01/28/2017, the [redacted] received a call from an [redacted] employee stating that PSP door [redacted] was [redacted].

Root Cause of Possible Violation:
• The pre-specification for PSP doors and door hardware is not detailed enough nor specific to the industrial security environment for which the doors exist.
• The pre-specification is not consistent throughout the PSP door fleet.
• A single vendor comprehensive industrial security approach to PSP door and door hardware maintenance and testing does not exist.
These root causes have resulted in high equipment variability and utilization of existing equipment that was not satisfactory for the industrial security environment. These conditions have led to multiple access control failures [redacted]) and high alarm volumes that consume [redacted] security resources and diminish awareness.

How was the violation discovered? Each of the five instances above were discovered by or reported to [redacted] who promptly notified the [redacted]

Timeline:
08/10/2016 at 8:52 am (Reported in [redacted]: [redacted] receipt and investigation of invalid attempt alarm for PSP door [redacted] Employee without valid authorized unescorted access swiped his badge at the PSP door then proceeded to pull the handle of the door and the door opened (physical access control failure).
08/18/2016 at 5:22 pm (Reported in [redacted]): [redacted] receipt and investigation of forced door alarm for PSP door [redacted] Contractor working outside PSP door was able to pull the door open without valid authorized access (physical access control failure).
01/20/2017 at 12:50:48 and again at 12:51:37: [redacted] receipt and investigation of an invalid attempt alarm followed by a forced door alarm for PSP door [redacted] The [redacted] was also able to open PSP door [redacted] from the outside without swiping his card (physical access control failure).
01/26/17: [redacted] receipt and investigation of door ajar alarm on PSP door [redacted]

Self Report

[redacted] (physical access control monitoring failure-lack of barrel bolt latch sensor).
01/28/2017: [redacted] receipt and investigation of a call from an [redacted] employee stating that PSP door [redacted] was [redacted] (physical access control failure).

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Mitigating Activities:
A PSP Door and Alarm Study was conducted on 02/10/2017 covering the [redacted] PSP doors at [redacted] One of the findings of the study included the identification of four high failure PSP doors that provide alternate access and make up a high percentage of alarms per month. Until the permanent solution is implemented, these alternate access PSP doors were temporarily blocked off on 02/13/2017 to reduce the high alarm volumes that consume [redacted] security resources.
Preventive Measures:
Standup on 02/02/2017 of bi-weekly conference call with [redacted] and [redacted] stakeholders to communicate and collaborate on [redacted] PSP door triage efforts until [redacted] led project plan is in place.
Commencing in early March, the [redacted] group assumed the lead in developing and executing a project plan to produce a detailed and consistent pre-specification for the [redacted] PSP doors and door hardware specific to the industrial security environment at [redacted] The project plan will also include the identification of a single vendor to implement a comprehensive industrial security approach to PSP door and door hardware maintenance and testing.
The work breakdown structure for the [redacted] project will act as milestone activities for this self-report's mitigation plan.

Date Mitigating Activities Completed: 2/13/2017

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 potential and actual impacts to the BPS are assessed to be a Violation Severity Level of "Severe."
[redacted] possesses detective controls that are effective in monitoring and responding to alerts, reports and/or discoveries of unauthorized physical access however, the preventive physical access controls for multiple PSP doors at [redacted] are failing and do not restrict access to Applicable Systems. These preventive control failures allow for opportunities to negatively impact the BES before detective controls are executed.

Risk Assessment of Impact to BPS: [redacted] identifies that the potential impact to the BES is high due to the high failure rate of preventive [redacted] PSP physical access controls.

[redacted] has not experienced 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:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017017304	CIP-006-6 R1.	

Mitigation Plan Submitted On: May 01, 2017

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: July 31, 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		
RFC2017017304	08/10/2016	CIP-006-6 R1.
Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.		

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

Summary of Violations
NOTE: The first two instances were previously reported on September 21, 2016 (NERC Violation ID: [redacted]. They are included in this self-report only to show the trend of door hardware failures occurring at [redacted]

Instance 1 (Reported in [redacted]: On 08/10/2016 at 8:52 am a [redacted] Physical Access Control System (PACS) invalid attempt alarm was received by the [redacted] ([redacted] for Physical Security Perimeter (PSP) door [redacted] Investigation of the alarm revealed an employee without valid authorized unescorted access swiped his badge at the PSP door then proceeded to pull the handle of the door and the door opened.

Instance 2 (Reported in [redacted] On 08/18/2016 at 5:22 pm a forced door alarm was received by the [redacted] for PSP door [redacted] Investigation of the alarm revealed that a contractor working outside of the PSP door was able to pull the door open without valid authorized access (swiping the badge).

Instance 3: On 01/20/2017 at 12:50:48 and again at 12:51:37 an employee without valid authorized unescorted access swiped her badge at [redacted] PSP door [redacted] Both attempts generated an invalid attempt alarm followed by a forced door alarm monitored by the [redacted] The employee was able to access PSP door [redacted] on the second attempt due to an intermittent door equipment failure. [redacted]

Instance 4: On 01/26/17 the [redacted] received a door ajar alarm on PSP door [redacted] PSP door [redacted] is a [redacted] During investigation of the alarm by a security officer, the door was pushed shut but the door ajar alarm would not clear. [redacted]

Instance 5: On 01/28/2017, the [redacted] received a call from an [redacted] employee stating that PSP door [redacted] was malfunctioning and [redacted]

Root Cause of Violations
• A single owner providing a comprehensive industrial security approach for PSP doors (providing oversight of PSP door security operations, maintenance and testing) does not exist.

• The pre-specification for PSP doors and door hardware is not detailed enough nor specific to the industrial security environment for which the doors exist.
• The pre-specification is not consistent throughout the PSP door fleet.

Scope Review (Extent of Condition)
The scope of this mitigation plan includes all [redacted] PSP doors and door hardware as the root causes listed apply to all existing equipment in the industrial security environment. The industrial environment conditions have led to multiple access control failures [redacted] and high alarm volumes that, due to the root causes listed, can affect any [redacted] PSP door.

Timeline
Date Event
08/10/2016 at 8:52 am Instance 1 (Previously reported in [redacted] receipt and investigation of invalid attempt alarm for PSP door [redacted] physical access control failure).
08/18/2016 at 5:22 pm Instance 2 (Previously reported in [redacted] receipt and investigation of forced door alarm for PSP door [redacted] Contractor working outside PSP door was able to pull the door open without valid authorized access (physical access control failure).
01/20/2017 at 12:50:48 and 12:51:37 Instance 3: [redacted] receipt and investigation of an invalid attempt alarm followed by a forced door alarm for PSP door [redacted] The [redacted] was also able to open PSP door [redacted] from the outside without swiping his card (physical access control failure).
01/26/17 Instance 4: [redacted] receipt and investigation of door ajar alarm on PSP door [redacted]
01/28/2017 Instance 5: [redacted] receipt and investigation of a call from an [redacted] employee stating that PSP door [redacted] was malfunctioning and [redacted] (physical access control failure).

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

Identification Mechanism
Each of the five instances were discovered by or reported to [redacted] who promptly notified 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:

Corrective Actions:
A PSP Door and Alarm Study (Milestone 1) was conducted on 02/10/2017 covering the [redacted] PSP doors at [redacted] and benchmarking other industrial sites to identify common equipment and human performance issues and resolutions. The study included an inventory of all [redacted] PSP door hardware, examination of all maintenance performed and re-examination of past violations regarding access control. The results of the study led to a two phased approach to implementing PSP door security operations, maintenance and testing for the [redacted] PSP doors:
• Phase 1: [redacted] most problematic doors
• Phase 2: Remaining [redacted] doors

Four PSP doors providing alternate access to [redacted] PSPs (ie. Not the primary entrance) were identified as high failure PSP doors during the Door and Alarm Study. These alternate access doors were temporarily roped off on 02/13/2017 with "Emergency Use Only" signs posted in an effort to reduce the high alarm volumes that consume [redacted] security resources (Milestone 2).

Preventive Actions:
• Define, document and communicate PSP Program roles and responsibilities to include Physical Security Program Owner accountability and business unit/vendor responsibilities as they relate to PSP operations and maintenance (Milestone 3).
• Develop Functional Requirements Document (FRD) to address business, functional, non-functional and stakeholder requirements for PSP doors and door hardware located in industrial security environments (Milestone 4).
• Develop a detailed pre-specification for PSP single door and double door design types. Pre-specifications will cover the door and associated door hardware for PSP doors located in industrial security environments (Milestone 5).
• Develop and execute a Pilot security operations and maintenance test plan for phase one PSP doors based on functional requirements and industrial design pre-specifications. Pilot Test Plan encompasses two standards: A PSP Single Door standard and PSP Double Door standard (Milestone 6).
• Conduct Test of One on PSP Single Door and PSP Double Door (Milestone 7) with the expected outcome of a 'Go-No Go' determination for implementing the Phase One PSP Door Replacement Plan for the [redacted] PSP doors and/or door hardware at [redacted] (Milestone 8) and Phase Two PSP Door Replacement Plan for the remaining [redacted] PSP doors and/or door hardware at [redacted] (Milestone 9).

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: July 31, 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
Milestone 1	Conduct PSP Door and Alarm Study. Study was conducted	02/10/2017	02/10/2017		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
	on all [redacted] PSP doors at [redacted] and included an inventory of all [redacted] PSP door hardware, examination of all maintenance performed and re-examination of past violations regarding access control. Other industrial sites were benchmarked as part of the study to identify common equipment and human performance issues and resolutions. A two phased approach will be taken to provide a comprehensive industrial security approach for [redacted] PSP doors: - Phase 1: [redacted] most problematic doors - Phase 2: Remaining [redacted] doors				
Milestone 2	Temporarily Block Off High Failure PSP Doors. [redacted] PSP doors providing alternate access to [redacted] PSPs (ie. Not the primary entrance) were identified as high failure PSP doors in the Door and Alarm Study. These alternate access doors have been temporarily roped off and "Emergency Use	02/13/2017	02/13/2017		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
	Only" signs were posted in an effort to reduce the high alarm volumes that consume [redacted] security resources.				
Milestone 4	Develop Functional Requirements Document (FRD). FRD will address business, functional, non-functional and stakeholder requirements for PSP doors and door hardware located in industrial security environments.	04/05/2017	04/05/2017		No
Milestone 6	Develop Pilot Test Plan. Develop and execute a Pilot security operations and maintenance test plan for phase one PSP doors based on functional requirements and industrial design pre-specifications. Pilot Test Plan encompasses two standards: A PSP Single Door standard and PSP Double Door standard.	04/09/2017	04/10/2017		No
Milestone 5	Develop PSP Door Pre-specifications. Develop a detailed pre-specification for PSP single door and double door design	04/10/2017	04/08/2017		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
	types. Pre-specifications will cover the door and associated door hardware for PSP doors located in industrial security environments.				
Milestone 7	Conduct Test of One on PSP Single Door and PSP Double Door. Expected outcome is a 'Go-No Go' determination for implementing Phase One PSP Door Replacement Plan and following Phase Two PSP Door Replacement Plan.	04/26/2017			No
Milestone 3	Define and Document PSP Program Roles and Responsibilities. Define, document and communicate PSP Program roles and responsibilities to include Physical Security Program Owner accountability and business unit/vendor responsibilities as they relate to PSP operations and maintenance.	05/31/2017			No
Milestone 8	Implement Phase One PSP Door Replacement Plan. Implement phase one replacement	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
	plan for the [redacted] PSP doors and/or door hardware at [redacted]				
Milestone 9	Implement Phase Two Rollout. Implement phase replacement plan for the remaining [redacted] PSP doors and/or door hardware at [redacted]	07/30/2017			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.

[redacted] PSP doors providing alternate access to [redacted] PSPs (ie. Not the primary entrance) were identified as high failure PSP doors during the Door and Alarm Study. These alternate access doors were temporarily roped off on 02/13/2017 with "Emergency Use Only" signs posted in an effort to reduce the high alarm volumes that consume [redacted] security resources (Milestone 2).

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 of [redacted] incurring further access control failures associated with the [redacted] PSP doors and door hardware located at [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

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: May 01, 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): RFC2017017304
Mitigated Standard Requirement(s): CIP-006-6 R1.
Scheduled Completion as per Accepted Mitigation Plan: October 13, 2017
Date Mitigation Plan completed: September 29, 2017
RF Notified of Completion on Date: October 13, 2017
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017304 Submission.zip	A Zip file "RFC2017017304 Submission.zip" contains the cover sheet for the whole package and supporting evidence for each milestone.	3,247,047

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 RFC2017017304

[redacted]

Standard/Requirement: CIP-006-6 R1

NERC Mitigation Plan ID: RFCMIT012854

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 03/17/17	05/01/17	05/26/17	06/28/17	10/13/17	09/29/17

Description of Issue

First instance: On 01/20/2017 at 12:50:48 and again at 12:51:37 an employee without valid authorized unescorted access swiped her badge at [redacted] PSP door [redacted] Both attempts generated an invalid attempt alarm followed by a forced door alarm monitored by the [redacted] The employee was able to access PSP door [redacted] on the second attempt due to an intermittent door equipment failure. [redacted]

[redacted]

Second instance: On 01/26/17 the [redacted] received a door ajar alarm on PSP door [redacted] PSP door [redacted] is a [redacted]

[redacted] The Alternate Measures Log was reviewed to verify that security was notified and alternate measures were put in place while the doors were propped open per [redacted] procedures.

Third instance: On 01/28/2017, the [redacted] received a call from an [redacted] employee stating that PSP door [redacted] was malfunctioning and [redacted]

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017017304 Submission	CIP-006-6 R1

Verification of Mitigation Plan Completion

Milestone 1: Conduct PSP Door and Alarm Study. Study was conducted on all [redacted] PSP doors at [redacted] and included an inventory of all [redacted] PSP door hardware, examination of all maintenance performed and re-examination of past violations regarding access control. Other industrial sites were benchmarked as part of the study to identify common equipment and human performance issues and resolutions. A two-phased approach will be taken to provide a comprehensive industrial security approach for 46 [redacted] PSP doors:

- Phase 1: [redacted] most problematic doors.

- Phase 2: Remaining [redacted] doors.

Proposed Completion Date: February 10, 2017

Actual Completion Date: February 10, 2017

File 1, "*RFC2017017304 Submission*", Milestone1 Submit, Page 2, shows the PSP door alarm study as indicated in milestone 1. This study produced evidence via data and analysis that uncontrollable environment variables was the root cause for the number of PSP door alarms associated with this systemic issue.

Milestone # 1 Completion verified

Milestone 2: Temporarily Block Off High Failure PSP Doors. [redacted] PSP doors providing alternate access to [redacted] PSPs (i.e. Not the primary entrance) were identified as high failure PSP doors in the Door and Alarm Study. These alternate access doors have been temporarily roped off and "Emergency Use Only" signs were posted in an effort to reduce the high alarm volumes that consume [redacted] security resources.

Proposed Completion Date: February 13, 2017

Actual Completion Date: February 13, 2017

File 1, "*RFC2017017304 Submission*" Milestone 2 Submit, Page, 2, shows a positive result of the entities' mitigation plan and actions taken after incident discovery. This document shows the number of nuisance alarms in which were generated prior to containment and countermeasures were effectively implemented. It shows the numbers in the thousands dropping to double digits almost immediately and then to the single digits within roughly 60 days' time.

Milestone # 2 Completion verified

Milestone 3: Define and Document PSP Program Roles and Responsibilities. Define, document and communicate PSP Program roles and responsibilities to include Physical Security Program Owner accountability and business unit/vendor responsibilities as they relate to PSP operations and maintenance.

Proposed Completion Date: May 31, 2017

Actual Completion Date: June 8, 2017

File 1, "*RFC2017017304 Submission*", Milestone3 Submit, Pages 2 through 6, illustrate the RACI model in which the entity created in order to identify responsibilities related to PSP Programs.

Milestone # 3 Completion verified

Milestone 4: Develop Functional Requirements Document (FRD). FRD will address business, functional, non-functional and stakeholder requirements for PSP doors and door hardware located in industrial security environments.

Proposed Completion Date: April 5, 2017

Actual Completion Date: April 5, 2017

File 1, "*RFC2017017304 Submission*", Milestone 4 Submit, Page 2, shows the functional requirements document which addresses stakeholder requirements residing within industrial security environments.

Milestone # 4 Completion verified

Milestone 5: Develop PSP Door Pre-specifications Develop a detailed pre-specification for PSP single door and double door design types. Pre-specifications will cover the door and associated door hardware for PSP doors located in industrial security environments.

Proposed Completion Date: April 10, 2017

Actual Completion Date: October 13, 2017

File 1, "*RFC2017017304 Submission*", Milestone 5 Submit, Pages 2 through 7, are an updated version of the entity [redacted] Access control hardware specifications. This document sets forth the entity standard based upon door classification as to what door specifications need to be followed and/ or addressed according to company policy and procedure. This Latest revision is effective October 13, 2017.

Milestone # 5 Completion verified

Milestone 6: Develop Pilot Test Plan. Develop and execute a Pilot security operations and maintenance test plan for phase one PSP doors based on functional requirements and industrial design pre-specifications. Pilot Test Plan encompasses two standards: A PSP Single Door standard and PSP Double Door standard.

Proposed Completion Date: April 10, 2017

Actual Completion Date: April 8, 2017

File 1, "*RFC2017017304 Submission*", Milestone 6 Submit, Pages 6 through 10, illustrate the pilot door test plan after the implementation of new hardware. This test plan proposed a specified and expected outcome to determine if the door passed/ failed. Based on Pages 7 through 10, it shows the expected outcome vs. the actual outcome and the remediation's if expected outcome was not obtained and/or failed.

Milestone # 6 Completion verified

Milestone 7: Conduct Test of One on PSP Single Door and PSP Double Door. Expected outcome is a 'Go-No-Go' determination for implementing Phase One PSP Door Replacement Plan and Following Phase Two PSP Door Replacement Plan.

Proposed Completion Date: April 26, 2017

Actual Completion Date: April 26, 2017

File 1, "*RFC2017017304 Submission*", Milestone 7 Submit, Pages 2 through 6, illustrate the actual door test plan after the implementation of new hardware. This test plan proposed a specified and expected outcome to determine if the door passed/ failed. Based on Pages 7 through 10, it shows the expected outcome vs. the actual outcome and the remediation's if expected outcome was not obtained and/or failed.

Milestone # 7 Completion verified

Milestone 8: Implement Phase One PSP Door Replacement Plan. Implement Phase on replacement plan for the [redacted] PSP doors and/or door hardware at [redacted]

Proposed Completion Date: June 30, 2017

Actual Completion Date: June 30, 2017

File 1, "*RFC2017017304 Submission*", Milestone 8 Submit, Pages 2 through 6, shows the first phase of the door replacement plan in regards to this milestone.

Milestone # 8 Completion verified

Milestone 9: Implement Phase Two Rollout. Implement phase replacement plan for the remaining [redacted] PSP doors and/or door hardware at [redacted]

Proposed Completion Date: October 13, 2017

Actual Completion Date: September 29, 2017

File 1, "*RFC2017017304 Submission*", Milestone 9 Submit, Page 4, shows the phase 2 replacement implementation including start and completion dates. As indicated by this milestone.

Milestone # 9 Completion verified

The Mitigation Plan is hereby verified complete.

Date: December 5, 2017

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-006-6
Requirement: CIP-006-6 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: May 01, 2017 **Changed to March 16, 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 March 16, 2017, [redacted] midnight [redacted] employees conducted a monthly [redacted] at all [redacted] Physical Security Perimeter (PSP) doors. These tests include testing for anything that could cause the door to send alarms, such as door forced, door propped and invalid access attempts. In the [redacted] one [redacted] PSP, it was identified that one [redacted] of two doors failed to alarm for both forced door and propped door. Alarms monitoring for invalid access attempts continued to function. Badge card readers continued to function properly. The failure was documented on the [redacted] barrier inspection form. No other actions were taken at that time. [redacted] process for barrier inspections includes documenting any failures on the barrier inspection form, creating a maintenance ticket in the [redacted] tool, activating alternate measures and maintaining alternate measures until repairs and retesting have been completed.
On April 10, 2017, [redacted] conducted an internal [redacted] and identified one barrier form for [redacted] indicating testing failures. The form was further investigated by [redacted] by checking for required maintenance tickets. [redacted] was unable to identify a maintenance ticket for the failure at [redacted] management conducted additional testing verifying that propped and forced door alarms were not being received at [redacted] Following [redacted] process alternate measures were activated and a maintenance ticket was created. [redacted] conducted initial maintenance by pushing configuration files to the system for [redacted] This action resulted in the door

resuming all alarming functions. Alternate measures were then ended and was notified of the potential violation.
On April 11, 2017, management reviewed configuration push conducted on and concluded the need for additional inspection by the door vendor. Alternate measures were activated and the door vendor was contacted. The vendor inspected the door and determined the root cause of the failure of the alarming function to be a wiring issue. Wires that were responsible for sending alarms were improperly installed and caused shortages due to improper insulation. The vendor made repairs to the door wiring at and inspected and made adjustments to wiring at the other door in the PSP in order to mimic wiring configuration at both doors. Both doors were tested and all alarming resumed functioning.
On April 17, 2017, Two employees received disciplinary action by the contracting agency. On April 20, 2017, following an investigation, one contract employee was removed from the position by the contract agency and the other contract employee was removed from the site.
On April 21, 2017, and conducted an at which time it was determined that alternate measures were no longer needed at

Root Cause of Possible Violation: The root cause of this violation was determined to be a human performance error. process for barrier inspections was not followed even though the employees were trained and had access to the process.

How was the violation discovered? The potential violation was discovered during an internal audit done by

Timeline:
March 16, 2017 - Barrier inspection conducted and alarm failure noted
April 10, 2017 - Internal Audit conducted on Alt barrier inspection form. Failures on inspection form identified and investigated
April 10, 2017 - Investigation resulted in the identification of alarming failures at
April 10, 2017 - Alternate measures activated, maintenance ticket created, initial maintenance performed, retesting conducted and alternate measure deactivated.
April 11, 2017 - management review. Determined vendor needed. Alternate measure activated. Vendor conducted investigation, made repairs and conducted retesting.
April 17, 2017 - Two contract employees disciplined
April 20, 2017 - One contract employee removed from and One contract employee removed from site.
April 21, 2017 - conducted and alternate measures deactivated.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Mitigating Activities:
On April 10, 2017, instituted alternate measures at the conformation of alarming failure.
On April 10, 2017, initial maintenance repair was conducted and retesting of PSP alarming function was conducted.
On April 11, 2017, management did a review of the incident and contacted the door vendor for further testing and repair. Alternate measures were activated.
On April 17, 2017, disciplinary action was issued for two contract employees which resulted in one contract employee being removed from and one contract employee being removed from the site.
On April 27, 2017, a physical walk down of the was conducted and no anomalies were found.
On April 28, 2017, to assess the extent of circumstances will conduct a review of all barrier logs for March 2017 to ensure

there were no additional failures identified and not escalated.

Preventive Measures:
To prevent any future reoccurrences, the vendor made repairs to door wiring at both doors in the [redacted] PSP and retested alarming functionality. [redacted] also conducts monthly barrier inspections at each [redacted] site.

Date Mitigating Activities Completed: April 28, 2017

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 BPS is severe following the VSL guidance. Additionally, there was the potential that a door could have been propped open and someone without proper authorization could have had access to the PSP.

The actual impact is low due to several mitigating factors in place during the potential violation. [redacted] has a layered protection approach to physical security at the [redacted] PSP. This [redacted] site first requires restricted access to the building and is continuously monitored by cameras. In addition, it is located approximately [redacted] feet from the [redacted] Badge reader functionality continued during the potential violation and monitoring for invalid access attempts at the PSP also continued to function. A walk down of the [redacted] PSP was completed on 04/27/2017 and no anomalies were found. [redacted] also has a process for maintenance and testing of PSP doors that requires testing to be performed monthly instead of biannually as required by CIP 006 R3.1.

Risk Assessment of Impact to BPS: The risk of Impact to the BPS has been identified as low due to the mitigating factors in place during the identification of the potential violation.

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: RFCMIT012890
Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017017547	CIP-006-6 R1.	

Mitigation Plan Submitted On: [redacted]
Mitigation Plan Accepted On:
Mitigation Plan Proposed Completion Date: May 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		
RFC2017017547	05/01/2017	CIP-006-6 R1.
Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.		

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

Brief Description: (What happened?)
On March 16, 2017, [redacted] ([redacted] employees conducted a monthly [redacted] at all [redacted] Physical Security Perimeter (PSP) doors. These tests include testing for anything that could cause the door to send alarms, such as door forced, door propped and invalid access attempts. In the [redacted] one [redacted] PSP, it was identified that one ([redacted] of two doors failed to alarm for both forced door and propped door. Alarms monitoring for invalid access attempts continued to function. Badge card readers continued to function properly. The failure was documented on the [redacted] barrier inspection form. No other actions were taken at that time. [redacted] process for barrier inspections includes documenting any failures on the barrier inspection form, creating a maintenance ticket in the [redacted] tool, activating alternate measures and maintaining alternate measures until repairs and retesting have been completed.
On April 10, 2017, [redacted] ([redacted] conducted an internal audit and identified one barrier form for [redacted] indicating testing failures. The form was further investigated by [redacted] by checking for required maintenance tickets. [redacted] was unable to identify a maintenance ticket for the failure at [redacted] management conducted additional testing verifying that propped and forced door alarms were not being received at [redacted] Following [redacted] process alternate measures were activated and a maintenance ticket was created. [redacted] conducted initial maintenance by pushing configuration files to the system for [redacted] This action resulted in the door resuming all alarming functions. Alternate measures were then ended and [redacted] [redacted] ([redacted] was notified of the potential violation.
On April 11, 2017, [redacted] [redacted] management reviewed configuration push conducted on [redacted] and concluded the need for additional inspection by the door vendor. Alternate measures were activated and the door vendor was contacted. The vendor inspected the door and determined the root cause of the failure of the alarming function to be a wiring issue. Wires that were responsible for sending alarms were improperly installed and caused shortages due to improper insulation. The vendor made repairs to the door wiring at [redacted] and inspected and made adjustments to wiring at the other door in the PSP in order to mimic wiring configuration at both doors. Both doors were tested and all alarming resumed functioning.
On April 17, 2017, Two [redacted] ([redacted] Contract employees received disciplinary action by the contracting agency. On April 20, 2017, following an investigation, one [redacted] contract employee was removed from the position by the contract agency and the other [redacted] contract employee was removed from the [redacted] site.
On April 21, 2017, [redacted] and [redacted] conducted an [redacted] at which time it was determined that alternate measures were no longer needed at [redacted]

Cause: (what caused the violation?)
The root cause of this violation was determined to be a human performance error. [redacted] process for barrier inspections was not followed even though the employees were trained and had access to the process.

How was the violation discovered?
The potential violation was discovered during an internal audit by [redacted]

Results of the RCA: (What is the root cause?)
The root cause of this violation was determined to be a human performance error.

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

This violation was identified during an internal audit conducted by [redacted]. Although there was a loss of forced and propped door alarming functionality at one door in the [redacted] PSP, alarming for invalid access attempts continued functioning during the entire violation period.

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] conducted a physical walk down of the [redacted] PSP. The purpose of this milestone is to check for any signs of tampering within the PSP. In this case no tampering was identified.

Milestone 2 - [redacted] conducted a review of all [redacted] barrier logs for the month of March 2017.The purpose of this milestone was to ensure that no other barrier inspections contained failures that were not escalated via the barrier inspection process. The result was that no other discrepancies were identified.

Milestone 3 - [redacted] provided alternate access control measures at the [redacted] PSP door. The purpose of this milestone was to ensure that during the time of alarming failure that no unauthorized personal gained access to the [redacted] PSP. The result was that alternate measures were in place during the period when alarms were not functioning.

Milestone 4 - [redacted] had the door vendor inspect and repair the door wiring at [redacted] in the [redacted] The purpose of this milestone is to identify cause for failure and fix wiring failure. The vendor inspected both doors in the Alternative [redacted] PSP and identified a fault in the door wiring at [redacted] which caused the alarming failure. [redacted] was repaired. The door wiring was changed at the other door in the PSP to mimic the door wiring at [redacted]

Milestone 5 - [redacted] validated that following the door wiring repairs that all alarming functionality was restored. The purpose of this milestone is to ensure functionality had returned. Functionality was validated.

Milestone 6 - [redacted] contract vendor disciplined two contract employees by removing one employee from [redacted] and removing one employee from duties at [redacted] PSP. The purpose of this milestone is to remediate the human performance error caused by the contract employees. The result was that the contract employees were disciplined.

Milestone 7 - [redacted] provided awareness communication to all staff responsible for maintenance and testing at all [redacted] facilities. The purpose of this milestone is to ensure that other employees responsible for maintenance and testing are aware of the proper procedures required

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: May 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
Repair Door wiring	[redacted] had the door vendor inspect and repair door wiring at [redacted] in the [redacted] The	04/11/2017	04/11/2017		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
	purpose of this milestone is to identify cause for failure and fix wiring failure.				
Verify alarming functionality	[redacted] validated that following door wiring repairs that all alarming functionality was restored. The purpose of this milestone is to ensure functionality has returned.	04/11/2017	04/11/2017		No
Discipline two contract employees	[redacted] contract vendor disciplined two contract employees by removing one employee from [redacted] and removing one employee from duties at [redacted] PSP. The purpose of this milestone is to remediated the human performance error caused by the contract employees.	04/20/2017	04/20/2017		No
Perform Alternate Measures	[redacted] provided alternate measures at the [redacted] PSP door. The purpose of this milestone is to ensure that during the time of alarming failure that no unauthorized personal gained access to the [redacted] PSP	04/26/2017	04/26/2017		No
Conduct Physical walk down of PSP	[redacted] conducted a physical walk down of the [redacted] PSP. The purpose of	04/28/2017	04/28/2017		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
	this milestone is to check for any signs of tampering within the PSP.				
Review all [redacted] barrier logs for March 2017	[redacted] conducted a review of all [redacted] barrier logs for the month of March 2017.The purpose of this milestone is to ensure that no other barrier inspections contained failures that were not escalated via the barrier inspection process.	[redacted]	04/28/2017		No
Reinforcement of procedures	[redacted] provided awareness of the maintenance and testing procedures to all staff responsible for maintenance and testing at all [redacted] facilities.	05/08/2017	05/08/2017		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 not identified any additional risk to the BPS. [redacted] maintains a robust testing and maintenance program that requires barrier inspection testing to be completed monthly at all [redacted] facilities. This practice is above and beyond the required bi-annual testing and is used to ensure proper maintenance of equipment at all [redacted] facilities. Additionally, at the time that the violation was identified it was confirmed that alarming for invalid access attempt continued to function and alternate measures were immediately instituted per the testing and maintenance program.

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 BPS 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. The wiring enhancements made to both doors in the [redacted] PSP will ensure wiring uniformity and functionality of all alarming. The discipline issued to two contract employees along with the to reinforce [redacted] commitment to the reliability and security of the BPS.

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): RFC2017017547
Mitigated Standard Requirement(s): CIP-006-6 R1.
Scheduled Completion as per Accepted Mitigation Plan: May 08, 2017
Date Mitigation Plan completed: May 08, 2017
RF Notified of Completion on Date: [redacted]
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017547 Certification.zip	The file "RFC2017017547 Certification.zip" contains: RFC2017017547 Certification cover page.pdf - cover page for overall package. Milestone 1 - Submit.pdf - evidence supporting milestone 1 Milestone 2- Submit.pdf - evidence supporting milestone 2 Milestone 3 - Submit.pdf - evidence supporting milestone 3 Milestone 4 - Submit.pdf - evidence supporting milestone 4 Milestone 5 - Submit.pdf - evidence supporting milestone 5 Milestone 6 - Submit.pdf - evidence supporting milestone 6 Milestone 7 - Submit.pdf - evidence supporting milestone 7	21,606,566
Entity	File 2 RFC2017017547 -		4,640,166

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Response to Milestone Questions.pdf		4,640,166
Entity	File 3 RFC2017017547 - Response questions cover.pdf		561,166
Entity	RFC2017017547 Updated milestones 4 5 and 6.zip	RFC2017017547 Updated milestones 4 5 and 6	48,754,776

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 RFC2017017547

[redacted]

Standard/Requirement: CIP-006-6 R1

NERC Mitigation Plan ID: RFCMIT012890

Method of Disposition: Settlement Agreement

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	05/08/17

Description of Issue

On March 16, 2017, [redacted] ([redacted] employees conducted a monthly [redacted] at all [redacted] Physical Security Perimeter (PSP) doors. These tests include testing for anything that could cause the door to send alarms, such as door forced, door propped and invalid access attempts. In the [redacted] one [redacted] PSP, it was identified that one ([redacted] of two doors failed to alarm for both forced door and propped door. Alarms monitoring for invalid access attempts continued to function. Badge card readers continued to function properly. The failure was documented on the [redacted] barrier inspection form. No other actions were taken at that time. [redacted] process for barrier inspections includes documenting any failures on the barrier inspection form, creating a maintenance ticket in the [redacted] tool, activating alternate measures and maintaining alternate measures until repairs and retesting have been completed.

On April 10, 2017, [redacted] ([redacted] conducted an internal audit and identified one barrier form for [redacted] indicating testing failures. The form was further investigated by [redacted] by checking for required maintenance tickets. [redacted] was unable to identify a maintenance ticket for the failure at [redacted] management conducted additional testing verifying that propped and forced door alarms were not being received at [redacted] Following [redacted] process alternate measures were activated and a maintenance ticket was created. [redacted] conducted initial maintenance

by pushing configuration files to the system for [redacted]This action resulted in the door resuming all alarming functions. Alternate measures were then ended and [redacted] was notified of the potential violation.

On April 11, 2017, [redacted] management reviewed configuration push conducted on [redacted] and concluded the need for additional inspection by the door vendor. Alternate measures were activated and the door vendor was contacted. The vendor inspected the door and determined the root cause of the failure of the alarming function to be a wiring issue. Wires that were responsible for sending alarms were improperly installed and caused shortages due to improper insulation. The vendor made repairs to the door wiring at [redacted] and inspected and made adjustments to wiring at the other door in the PSP in order to mimic wiring configuration at both doors. Both doors were tested and all alarming resumed functioning.

On April 17, 2017, Two [redacted] Contract employees received disciplinary action by the contracting agency. On April 20, 2017, following an investigation, one [redacted] contract employee was removed from the position by the contract agency and the other [redacted] contract employee was removed from the [redacted] site. On April 21, 2017, [redacted] and [redacted] conducted an [redacted] at which time it was determined that alternate measures were no longer needed at [redacted]

The root cause of this violation was determined to be a human performance error. [redacted] process for barrier inspections was not followed even though the employees were trained and had access to the process.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017017547 Certification	CIP-006-6 R1
File 2	RFC2017017547 Response to Milestone Questions	CIP-006-6 R1
File 3	RFC2017017547 Response questions cover	CIP-006-6 R1
File 4	RFC2017017547 Updated Milestone 4, 5 and 6	CIP-006-6 R1

Verification of Mitigation Plan Completion

Milestone 1: Repair Door wiring.

File 1, "*RFC2017017547 Certification*", Milestone 1 Submit, Pages 2 and 3, show a detailed bill from the vendor ([redacted]) describing that they were contacted to perform a troubleshooting and repair on the entity doors as indicated in this milestone.

Milestone # 1 Completion verified.

Milestone 2: Verify alarming functionality.

File 1, "*RFC2017017547 Certification Package*", Milestone 2 Submit, Pages 2 through 7, show the testing results of the door functionality after repair and prior to placing the door back into service.

Milestone # 2 Completion verified.

Milestone 3: Discipline two contract employees.

File 1, "*RFC2017017547 Certification Package*", Milestone 3 Submit, Page 1, is a description of the disciplinary action that was taken while Page 2 is a signed attestation stating that disciplinary action was taken.

Milestone # 3 Completion verified.

Milestone 4: Perform Alternate Measures.

File 4, "*RFC2017017547 Updated Milestone 4, 5 and 6*", Milestone 4 Submit update Pages 1 through 9, and information provided via teleconference show the alternate measures log along with a description of how/ what these alternate measures are and how they were carried out. [redacted] The blanks within the evidence are also part of this mitigation plan and the entity did take immediate corrective actions for security officers who did not complete the logs as required.

Milestone #4 Completion verified.

Milestone 5: Conduct Physical walk down of PSP.

File 4, "*RFC2017017547 Updated Milestone 4, 5 and 6*", Milestone 5 submit update, Pages 2 through 27, show the updated tampering verification log which was discussed in detail via a teleconference with entity staff in regards to ensuring that they are/ were checking for signs of

physical and electronic tampering. Since the teleconference the entity has changed its procedures and policies in order to reflect the checks for electronic and physical checks when in regards to tampering.

Milestone # 5 Completion verified.

Milestone 6: Review all [redacted] barrier logs for March 2017.

File 4, "*RFC2017017547 Updated Milestone 4, 5 and 6*", Milestone 6 submit update, Pages 2 through 45, provide Q&A responses from RF to entity in regards to this mitigation plan as well as the testing log with additional callouts that were discussed via teleconference with the entity. The entity has provided additional callouts as to the blank areas in the logs and have since made corrections to their documentation in order to account for items that are not applicable (N/A) instead of leaving them blank and incomplete. This evidence provides account for their door testing sequence and the previous teleconference provided insight into how this testing is conducted.

Milestone # 6 Completion verified.

Milestone 7: Reinforcement of procedures.

File 1, "*RFC2017017547 Certification Package*", Milestone 7 Submit, Pages 2 and 3, show the training topics and the attendees of the training required by milestone 7.

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-006-6
Requirement: CIP-006-6 R1.
Date Submitted: August 03, 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 25, 2017
End/Expected End Date: June 19, 2017
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: The [redacted] computer room at the [redacted] contains the following eight Bulk Electric System cyber assets:

ID	Description	Classification
[redacted]		

The exposure was discovered on 6/19/2017 at around 11 am. [redacted] No one has reported anything missing or that any equipment has been tampered with.

Self Report

All PSPs inspected during the walk down were intact expect [redacted] PSP.

The exposure was fixed immediately by end of the same day as discovery, 6/19/2017.

Root Cause of Possible Violation:
[redacted] organization, leading the construction project, was unaware if the construction affects a Physical Security Perimeter (PSP) or is adjacent to a PSP.

How was the violation discovered?
During a NERC walk down, white powder was noticed on the computer room floor at the wall.

Timeline:
9/13/2016: Last walk down of computer room by [redacted] and [redacted] NERC CIP staff. No sign of PSP damage existed.
5/25/2017: [redacted]
6/19/2017 approximately 11 am: Exposure discovered during walk down of computer room.
6/19/2017 end of day: Exposure eliminated - [redacted]

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Mitigating Activities:
7/25/2017: Per walk down conducted on 7/25/17, verified that no tampering of the hardware occurred during the period May 25 through July 25.
8/3/2017: Per review of system logs, verify that no breach occurred in the software during the period May 25 through June 19.

Preventative Measures:
6/20/2017: [redacted]
8/18/2017: Update and disseminate [redacted] procedures to address NERC CIP requirements for cyber assets, including informing [redacted]

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 BPS is Severe, as [redacted] has documented and implemented physical access controls, but at least one control did not exist to restrict access to applicable systems.

The actual impact to the BPS is Lower, as it was verified there were no breaches of the software nor tampering of the hardware during the period of exposure, and the exposure has been eliminated with access to the [redacted] now blocked. In addition, physical access to [redacted] is required and this PSP is two layers deep in bigger scheme of physical security at [redacted]

Risk Assessment of Impact to BPS:

The potential impact to the BPS is Lower, as it was verified there was no breach of the software nor tampering of the hardware, and the exposure has been eliminated.

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:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017018166	CIP-006-6 R1.	

Mitigation Plan Submitted On: September 08, 2017

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: November 17, 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		
RFC2017018166	05/25/2017	CIP-006-6 R1.
Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.		

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

Brief Description: (What happened?)
The [redacted] computer room at the [redacted] contains the following eight Bulk Electric System cyber assets:

[redacted]

[redacted] Hence violation of CIP006-6 R1 Part 1.2.

The exposure was discovered on 6/19/2017 at around 11 am. [redacted] No one has reported anything missing or that any equipment has been tampered with.

All PSPs inspected during the walk down were intact except [redacted] PSP.

The exposure was fixed immediately by end of the same day as discovery, 6/19/2017.

The physical security perimeter ("PSP") of the [redacted] computer room at the [redacted] PP was broken when [redacted]

Cause: (what caused the violation?)
[redacted]

Results of the [redacted] (What is the root cause?)
[redacted] organization, leading the construction project, was unaware if the construction affects a Physical Security Perimeter (PSP) or is adjacent to a PSP.

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

During a NERC walk down on June 19, 2017, [redacted] holes in them where light was shining through.

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 - Walk down the PSP to verify that no tampering, a visual inspection to validate that there are no dongles or USB devices plugged into the cyber asset hardware, occurred since the exposure on May 25, 2017. All PSPs inspected during the walk down were intact except [redacted] PSP. [redacted] As soon as the exposure was discovered, the [redacted] team worked with the construction contractor to address the problem. The exposure was fixed immediately by end of the same day as discovery, 6/19/2017. [redacted]

Milestone 2 - Update and disseminate [redacted] ([redacted] procedures, to address NERC CIP requirements for cyber assets. The purpose of this milestone is to ensure that all Project Managers with [redacted] are aware of and account for NERC CIP assets in their direct project plans as well as any ancillary areas that may be in contact with their projects. The following Preventive Measures have been put in place:
- [redacted] has been revised to include an item under the General Section that states:
If this is a NERC Regulated Site, contact [redacted] and site Cyber SME to determine if this affects a Physical Security Perimeter (PSP) or is adjacent to a PSP.

- [redacted] has been revised to include an agenda item that states:
Potential NERC/CIP Impact (Y/N) (If Yes, complete Construction Checklist [redacted] Required Actions.

Milestone 3 - Determine baselines and review [redacted] logs to verify that no tampering of the cyber asset software occurred during the period May 25, 2017 through June 19, 2017.

Milestone 4 - The record documents, which entail plans and schematics, will be updated when the project is completed. We anticipate the updates to take place by November 17, 2017. The updating of these records will help to ensure in future construction projects that the plenum block will remain intact.

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 17, 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
Verify no tampering of the hardware	Walk down the PSP to verify that no	07/25/2017	07/25/2017		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
	tampering of the cyber asset hardware occurred since the exposure on May 25				
Update [redacted] procedures	Update and disseminate [redacted] procedures to address NERC CIP requirements for cyber assets	07/27/2017	07/27/2017		No
Verify no tampering of the software	Determine baselines and review [redacted] (' [redacted] logs to verify that no tampering of the cyber asset software occurred during the period May 25, 2017 through June 19, 2017	08/18/2017	08/18/2017		No
Update records documents	The records documents, which entail plans and schematics, will be updated to include [redacted] to prevent [redacted] access.	11/17/2017			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 risk is minimal since the area that was exposed has been fixed by blocking the [redacted] as of the end of the day on June 19, 2017. The access to this PSP is controlled by badge access. Therefore, compensating controls are in place that would have prevented a greater impact to the 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

By updating and disseminating [redacted] procedures to address NERC CIP requirements for cyber asset, including informing [redacted] the initial Agenda has been updated to include a checklist item "Potential NERC/CIP Impact (Y/N). (If yes, complete Construction Checklist [redacted]" The addition of this item now brings attention to this area and any new construction/remodeling projects are now aware of the requirement and projects will contain contingencies if NERC CIP requirements for cyber assets are involved directly or indirectly.

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 08, 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): RFC2017018166
Mitigated Standard Requirement(s): CIP-006-6 R1.
Scheduled Completion as per Accepted Mitigation Plan: November 17, 2017
Date Mitigation Plan completed: November 17, 2017
RF Notified of Completion on Date: November 17, 2017
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017018166 Certification Package.zip	Attached ZIP file contains the cover sheet of the package and also the supporting evidence of each milestone.	16,449,212

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 RFC2017018166

[redacted]

Standard/Requirement: CIP-006-6 R1

NERC Mitigation Plan ID: RFCMIT013214

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 08/03/17	09/08/17	10/04/17	10/26/17	11/17/17	11/17/17

Description of Issue

[redacted]

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017018166 Certification Package	CIP-006-6 R1

Verification of Mitigation Plan Completion

Milestone 1: Verify no tampering of the hardware.

Proposed Completion Date: July 25, 2017

Actual Completion Date: May 25, 2017

File 1, "*RFC2017018166 Certification Package*", Milestone 1- Submit, Pages 2 through 6, show the results of the physical walk-down to verify that there was no tampering of assets physically.

Milestone # 1 Completion verified.

Milestone 2: Update [redacted] procedures.

Proposed Completion Date: July 27, 2017

Actual Completion Date: July 27, 2017

File 1, "*RFC2017018166 Certification Package*", Milestone 2- Submit, Pages 2 through 20, provide documentation particularly a checklist (Page 3 section 7) in regards to contacting [redacted] and a cyber SME in the event that a PSP and or adjacent location will be affected. In addition, new instruction for notifying construction managers was sent out to affected parties to notify them of procedural changes in this regard.

Milestone # 2 Completion verified.

Milestone 3: Verify no tampering of the software.

Proposed Completion Date: August 18, 2017

Actual Completion Date: August 18, 2017

File 1, "*RFC2017018166 Certification Package*", Files 3- Submit, Page 5 through 116, shows the [redacted] results of the affected assets showing that no deviation from the existing baseline existed.

Milestone # 3 Completion verified.

Milestone 4: Update records documents.

Proposed Completion Date: November 17, 2017

Actual Completion Date: November 6, 2017

File 1, "*RFC2017018166 Certification Package*", Milestone 4- Submit, Page 2, shows the architectural drawing showing [redacted] in order to prevent access as determined by this milestone in regards to updating the records and documents.

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-006-6

Requirement: CIP-006-6 R1.

Date Submitted: December 14, 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: November 28, 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: Incident description

On November 28, 2017 at approximately, 4:41 PM, the [redacted] ([redacted] at the [redacted] received an "Invalid Access Attempt" and an immediate second alarm for "Forced entry" from card reader [redacted] (Door of [redacted] PSP).

[redacted] immediately responded to these alarms and when the physical security team reached onsite they confirmed that employee ID that had triggered the invalid access attempt was a [redacted] employee with authorized unescorted access to the area. However, the employee was carrying multiple cards along with his [redacted] door access card, the card reader read FOB for his gym access. The card reader denied access and alerted an Invalid access to the [redacted] This indicates that the card reader was working as required and the Invalid access attempt alert was appropriate. Despite denied access, the door could be pulled open by the employee, who did not realize the access was denied. This triggered the second alarm at [redacted] for Forced entry.

On investigation by the security personal, the door's locking mechanism was malfunctioning and was not locking into place. The employee was therefore able to pull open the door despite a denied access with the Key FOB.

The security personal who attended to the alarm had seen a video preview of the employee to confirm the incidents causing the alarm. He performed a

preventive maintenance on the door immediately following the incident, including degreasing the lock that was preventing it from falling into correct locking mechanism and ensuring the latch was functioning as required following the incident.

[redacted] such doors exist at the [redacted] To check extent of condition, [redacted] reviewed the alarm logs for all [redacted] doors since last inspection of the doors to ensure that no forced entry alarm had been recorded from any of the doors. It was confirmed this was the only incident of such a nature.

What is the problem?
A malfunctioning door at [redacted] opened despite an invalid access by the card read for door # [redacted]
The user had authorized unescorted physical access, since the user entry into the PSP was not logged, this has been recorded as a violation of CIP-006- R1 P1.8 - "Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry."

Root Cause of Possible Violation:
As per the [redacted] & RCA performed on 12/08/2017, the door locking mechanism malfunctioned and did not secure the lock in the desired place due to lack of a maintenance program

How was the violation discovered?
On 11/28/2017, the [redacted] ([redacted] at the [redacted] received an Invalid Access Attempt and an immediate second alarm for Forced entry from card reader # [redacted] Further investigation by the physical security team, determined valid unescorted access for the employee but a malfunctioning door that did not lock into place allowing for forced entry alarm.

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 the door malfunctioning i.e. technical problem, due to lack of a maintenance program at the [redacted] [redacted]

Timeline:
1. 28 November 2016 - the [redacted] ([redacted] at the [redacted] [redacted] received an Invalid Access Attempt and an immediate second alarm for Forced entry from card reader # [redacted]
2. 28 December 2016 - A member of the Security team, reviewed the 2 alarms on video and then reached on-site to discuss incident with employee who had triggered the alarm to confirm authorized unescorted access card of the employee , and an invalid Fob swiped by the employee instead of the valid [redacted] card in error.
3. 28 December 2016 - This member of the security team, examined the door locking magnetic bars and noticed they were not latching as required. He performed a degreasing of the lock and ensured the locking mechanism worked securely before leaving the site.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure:

Corrective (Immediate) Activities:
An immediate corrective maintenance on door with card reader # [redacted] was performed following the incident to ensure the door's locking mechanism was working as required. It was checked and corrected to secure entry.

Mitigating Activities:
To Counter the invalid access alarms as a false occurrence, due to multiple cards (such as key fobs and access cards together), a broadcast

Self Report

communication will be circulated to all [redacted] Employees by 12/15/2017 to ensure they carry their door access cards separate from other readable electronic chips that might cause an Invalid Access Attempt alarms.

Alarm log for forced-in and forced-out instances for all [redacted] doors was reviewed for similar forced entry alarms to ensure no malfunctioning of the door mechanism could have caused a potential insecure unlogged entry into the PSP. The logs were reviewed since the last reported inspection performed at the door. No such incident was identified in this review.

Preventative Measures:
To ensure that the doors functions as required, a maintenance contract with a service provider for all [redacted] doors located in the [redacted] will be finalized by 12/31/2017. This maintenance would include maintenance and repair to avoid malfunctioning of the doors, including the locking mechanism.

Once the maintenance contract is finalized, the details of the contract would be entered into a [redacted] WO to monitor the Project Management of the execution of the contract for all doors.

A SWI for the maintenance program of the doors will be created.

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
Since the user had authorized unescorted access granted to the PSP, his entry into the door did not cause any risk. The door logs were also reviewed since last inspection to check for similar forced alarm entries. Post review, it was confirmed that there are no alarms since last inspection.

Potential Impact
Potential impact of a forced entry alarm to a PSP was low since the user had authorized unescorted access and was a daily worker in the [redacted]

Risk Assessment of Impact to BPS:
The risk assessed to the BES is low based on access level of the employee who triggered the alarm and a review of all alarm logs at [redacted] to determine no such incident that been recorded for door malfunctioning causing a forced door alarm since last inspection performed on the doors in December 6, 2017.

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:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017018857	CIP-006-6 R1.	

Mitigation Plan Submitted On: January 08, 2018

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: January 12, 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		
RFC2017018857	11/28/2017	CIP-006-6 R1.
Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.		

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

On November 28, 2017 at approximately, 4:41 PM, the [redacted] ([redacted] at the [redacted] received an "Invalid Access Attempt" and an immediate second alarm for "Forced entry" from card reader #[redacted] (Door of [redacted] PSP).
[redacted] immediately responded to these alarms and when the physical security team reached onsite they confirmed that employee ID that had triggered the invalid access attempt was a [redacted] employee with authorized unescorted access to the area. However, the employee was carrying multiple cards along with his [redacted] door access card, the card reader read FOB for his gym access. The card reader denied access and alerted an Invalid access to the [redacted] This indicates that the card reader was working as required and the Invalid access attempt alert was appropriate. Despite denied access, the door could be pulled open by the employee, who did not realize the access was denied. This triggered the second alarm at [redacted] for Forced entry.
On investigation by the security personnel, the door's locking mechanism was malfunctioning and was not locking into place. The employee was therefore able to pull open the door despite a denied access with the Key FOB. The security personnel who attended to the alarm had seen a video preview of the employee to confirm the incidents causing the alarm. He performed a preventive maintenance on the door immediately following the incident, including degreasing the lock that was preventing it from falling into correct locking mechanism and ensuring the latch was functioning as required following the incident.
[redacted] [redacted] such doors exist at the [redacted] To check extent of condition, [redacted] [redacted]reviewed the alarm logs for all [redacted] doors since last inspection of the doors to ensure that no forced entry alarm had been recorded from any of the doors. It was confirmed this was the only incident of such a nature.
What is the problem?
A malfunctioning door at [redacted] opened despite an invalid access by the card read for door # [redacted]
The user had authorized unescorted physical access, since the user entry into the PSP was not logged, this has been recorded as a violation of CIP-006- R1 P1.8 - "Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry."
Root Cause of Possible Violation:
As per the [redacted] & RCA performed on 12/08/2017, the door locking mechanism malfunctioned and did not secure the lock in the desired place due to lack of a maintenance program
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 the door malfunctioning i.e. technical problem, due to lack of a maintenance program at the [redacted] [redacted]
*Timeline:
1. 28 November 2016 - the [redacted] ([redacted] at the [redacted] received an Invalid Access Attempt and an immediate second alarm for Forced entry from card reader #[redacted]
2. 28 December 2016 - A member of the Security team, reviewed the 2 alarms on video and then reached on-site to discuss incident with employee who had triggered the alarm to confirm authorized unescorted access card of the employee , and an invalid Fob swiped by the employee instead of the valid [redacted] card in error.
3. 28 December 2016 - This member of the security team, examined the door locking magnetic bars and noticed they were not latching as required. He performed a degreasing of the lock and ensured the locking mechanism worked securely before leaving the site.

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

On 11/28/2017, the [redacted] ([redacted] at the [redacted] received an Invalid Access Attempt and an immediate second alarm for Forced entry from card reader #[redacted] Further investigation by the physical security team, determined valid unescorted access for the employee but a malfunctioning door that did not lock into place allowing for forced entry alarm.

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:

Mitigating Activity:
Milestone 1: Review alarm log for forced-in and forced-out instances for all [redacted] doors. Purpose of this milestone is to verify that the similar condition did not exist on any other door. The review was performed for the period of last inspection to current date. All the doors were found functioning without any issues. This review was performed by [redacted] analyst in [redacted] The evidence will be review of logs for all the PSP doors in [redacted]

Preventative activities: The milestones below directly address the root cause and help reduce the risk of such occurrences in future.

Milestone 2: A SWI for the maintenance program of the doors will be created. Purpose of this SWI is to help the assignee of the WO to perform the work.

Milestone 3: The WO is a required artifact to perform any and all the jobs in [redacted] In order to [redacted] the mitigation, [redacted] will create a recurring Work Order (WO) in [redacted] for monthly maintenance of all PSP doors. Purpose of this milestone is to ensure that every month a WO is assigned by the system (no human interaction) without a failure. The assignee will perform the work and will have to close the WO otherwise [redacted] will create an automatic escalation.

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 12, 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
Review alarm log for forced-in and forced-out instances for all [redacted] doors.	Purpose: Ensure that a similar condition does not exist on any other door. Evidence: An excel sheet with review from [redacted]	12/13/2017	12/13/2017		No
Develop SWI for the maintenance program of the doors	Purpose: Help the assignee of the WO to perform the work. Evidence: A newly created SWI	12/21/2017	12/21/2017		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
Create a recurring Work Order (WO) in [redacted] for monthly maintenance of all PSP doors	Purpose: Ensure that WO is issued and Preventive Maintenance is performed. The SWI noted in last milestone is reviewed/provided as Pre-Specification with monthly WO. Evidence: A recurring [redacted] Work Order	01/12/2018			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.

Based on the review of logs of all the doors [redacted] does not see any risk or a negative impact as all other doors functioned without a failure. All the processes and procedures for alarming, alerting [redacted] and performing an immediate preventive maintenance worked as designed.

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

A monthly preventive maintenance will reduce the risk of occurrence of similar issues in future.

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

This activity was completed on 12/08/2017.
Communicate to all the employees in the [redacted] advising them to carry the door access key separate from other access cards or key fobs. Purpose of this milestone to raise the awareness that the non [redacted] "electronically readable" cards/fobs may create noise when used along with [redacted] door access card.

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 08, 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): RFC2017018857
Mitigated Standard Requirement(s): CIP-006-6 R1.
Scheduled Completion as per Accepted Mitigation Plan: January 12, 2018
Date Mitigation Plan completed: January 05, 2018
RF Notified of Completion on Date: January 31, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017018857 Certification Package.zip	Zip file "RFC2017018857 Certification Package" contains cover page for the package and also supporting evidence for each milestone.	1,839,982

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 RFC2017018857

[redacted]

Standard/Requirement: CIP-006-6 R1

NERC Mitigation Plan ID: RFCMIT013482

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report 12/14/17	01/08/18	01/30/18	02/15/18	01/31/18	01/09/18

Description of Issue

On November 28, 2017 at approximately 4:41 PM, the [redacted] ([redacted] at the [redacted] received an "Invalid Access Attempt" and an immediate second alarm for "Forced entry" from card reader #[redacted] (Door of [redacted] PSP).

[redacted] immediately responded to these alarms and when the physical security team arrived onsite they confirmed that employee ID that had triggered the invalid access attempt was a [redacted] employee with authorized unescorted access to the area. However, the employee was carrying multiple cards along with his [redacted] door access card, the card reader read FOB for his gym access. The card reader denied access and alerted an Invalid access to the [redacted] This indicates that the card reader was working as required and the Invalid access attempt alert was appropriate. Despite denied access, the door could be pulled open by the employee, who did not realize the access was denied. This triggered the second alarm at [redacted] for Forced entry.

The door's locking mechanism was malfunctioning and was not locking into place. The employee was therefore able to pull open the door despite a denied access with the Key FOB. The security personnel performed preventive maintenance on the door immediately following the incident, including degreasing the lock that was preventing it from falling into correct locking mechanism and ensuring the latch was functioning as required following the incident.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2017018857 Certification Package	CIP-006-6 R1
File 2	[redacted] RFC2017018857 Additional questions Response	CIP-006-6 R1
File 3	RFC2017018857 Additional Data on request	CIP-006-6 R1

Verification of Mitigation Plan Completion

Milestone 1: Review alarm log for forced-in and forced-out instances for all [redacted] doors.

Proposed Completion Date: December 13, 2017

Actual Completion Date: October 26, 2017

File 1, "*RFC2017018857 Certification Package*", Milestone1- Submit, Pages 1 through 4, show that door alarm log was reviewed. This item provides a sampling of the door records that were reviewed out of the [redacted]

Additional information provided via Data request. File 3, "*RFC2017018857 Additional Data on request*", file containing Milestone 3- Submit, Pages 1 through 10, contains additional door samples that yielded no negative results per request and per milestone 1.

Milestone # 1 Completion verified.

Milestone 2: Develop SWI for the maintenance program of the doors.

Proposed Completion Date: December 21, 2017

Actual Completion Date: January 9, 2018

File 1, "*RFC2017018857 Certification Package*", Milestone 2- Submit, Pages 4 through 10, which is a work instruction describing preventative maintenance in regards to CIP doors as determined in this milestone.

Milestone # 2 Completion verified.

Milestone 3: Create a recurring Work Order (WO) in [redacted] for monthly maintenance of all PSP doors.

Proposed Completion Date: January 12, 2018

Actual Completion Date: December 16, 2017

File 3, "*RFC2017018857 Additional Data on request*", Milestone 3- Submit Page 3, shows the tasks created until April in order to maintain the doors as required by this milestone. Page 2 shows the configuration of that [redacted] work order showing its frequency and frequency units.

Milestone # 3 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: March 10, 2018

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Attachment 8

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

8.a The Entity's Self-Report (RFC2016016341);
8.b ReliabilityFirst's Verification of Mitigating Activities Completion dated [redacted];
8.c The Entity's Self-Report (RFC2016016342);
8.d The Entity's Mitigation Plan designated as RFCMIT012397-1 submitted [redacted];
8.e The Entity's Certification of Mitigation Plan Completion dated [redacted];
8.f ReliabilityFirst's Verification of Mitigation Plan Completion dated [redacted]

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-007-6 **Changed to CIP-007-3a R3**

Requirement: CIP-007-6 R2.

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 February 9, 2015**

End/Expected End Date: October 05, 2016

Region Initially Determined a Violation On:

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 January 9, 2015 [redacted] released a [redacted] Patch addressing the following vulnerabilities within the [redacted]:

[redacted]

The recommended solution was "to upgrade to [redacted] as part of your normal patch management cycle".
The [redacted] servers ([redacted] in [redacted] environment were affected by the [redacted] vulnerability due to a custom version of [redacted] running on them. This release was issued outside [redacted] normal patch release process (i.e. [redacted]).The [redacted] SME installed the [redacted] patch on [redacted] servers on August 17, 2016 ([redacted]) without a formal evaluation of the patch.

The root causes was determined to be process gap (process did not consider off-cycle patching).

Mitigating Activities:

Self Report

Description of Mitigating Activities and Preventative Measure: Mitigating Activities: All other patches released by [redacted] using standard release process (i.e. [redacted]) were evaluated and the applicable patches were applied to the systems or included in a mitigation plan.

Preventative Measures:
1) the patching process was updated to include off-cycle patching notifications,
2) the patch was applied, and
3) Patching-[redacted] were conducted by Business Unit and will included all employees involved in patching.

Date Mitigating Activities Completed: October 05, 2016

Impact and Risk Assessment:

Potential Impact to BPS: Moderate

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: The Potential and Actual Impact to the BES is low. To exploit any of the four vulnerabilities, the individual needs to be inside the network and have access to the [redacted] server.

Risk Assessment of Impact to BPS: [redacted] identifies that that potential impact to the BES is low. [redacted] has not experienced any negative impact 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			

Mitigating Activities Verification for RFC2016016341

[redacted]

Standard/Requirement: CIP-007-6 R2 **Changed to CIP-007-3a R3**

NERC Registry ID: [redacted]

Method of Disposition: Not yet determined

Relevant Dates			
Initiating Document	**Submittal of Activities**	**RF Acceptance**	**Date of Completion**
Self-Report [redacted]	[redacted]	[redacted]	10/05/16

Description of Issue

On January 9, 2015 [redacted] released a [redacted] Patch addressing the following vulnerabilities within the [redacted]:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

The recommended solution was to upgrade to [redacted] as part of [redacted] normal patch management cycle.

The [redacted] servers ([redacted] in [redacted] environment were affected by the [redacted] vulnerability due to a custom version of [redacted] running on them. This release was issued outside [redacted] normal patch release process (i.e. [redacted] report).The [redacted] SME installed the [redacted] patch on [redacted] servers on August 17, 2016 ([redacted]) without a formal evaluation of the patch.

The root causes was determined to be process gap (process did not consider off-cycle patching).

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2016016431- Additional Information	CIP-007-6 R2
File 2	Mitigating Activities	CIP-007-6 R2

Verification of Mitigation Plan Completion

Milestone 1: All other patches released by [redacted] using the standard release process (i.e. [redacted]) were evaluated and the applicable patches were applied to the systems or included in a patching mitigation plan as of September 9, 2016.

File 1, "*RFC2016016431- Additional Information*", Pages 2 through 27, illustrate the evidence that was previously missing showing the [redacted], evaluation of patches and whether they were installed or not. If not, this document shows their disposition and explanation as to why patches could not be installed.

Milestone # 1 Completion verified.

Milestone 2: The patching process was updated to include off-cycle patching notifications.

File 2, "Mitigating Activities", MA 1) [redacted]6 R2 Patch Management SWI, Pages 3 and 4, sections 2.1.1 through 2.1.4 illustrate the entity's new process for patch evaluation. This update process previously created July 21, 2016 and was the reason that the entity successfully found this incident.

Milestone # 2 Completion verified.

Milestone 3: The [redacted] patch was applied.

File 2, "*Mitigating Activities*", MA 2 CO 23976, pages 1 through 2 show the change order in which the entity deployed (page 1) and installed (Page 2) the [redacted] patch.

Milestone # 3 Completion verified.

Milestone 4: Patching compliance- [redacted] were conducted by Business Unit that included all employees involved in patching by October 5, 2016.

File 2, "*Mitigating Activities",* MA 3a) Patch Management Program Compliance Stand- FINAL, Pages 1 through 3, show the topics covered by the entity in their [redacted] meetings.

File 2, "*Mitigating Activities*", MA 3b) [redacted] – [redacted] PMP [redacted] Meeting Sign-in sheet, Page 1 shows the [redacted] departments sign in sheet for the previously mentioned stand-down.

File 2, "*Mitigating Activities*", MA 3c) [redacted] 20161006064118581, Page 1, shows the [redacted] facility sign in sheet for the previously mentioned [redacted]

File 2, "*Mitigating Activities*", MA 3d) Network Eng – Oct5 NERC CIP patching [redacted] sign in sheet, Page 1, shows the [redacted] sign in sheet for the previously mentioned stand-down.

File 2, "*Mitigating Activities*", MA 3e) [redacted] patching [redacted] Page 1, shows the [redacted] department sign in sheet for the previously mentioned [redacted]

Milestone #4 Completion verified.

The Mitigating Activities is hereby verified complete.

Date: [redacted]

Kristen Senk
Senior Counsel
ReliabilityFirst Corporation

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-007-6

Changed to CIP-007-3a R3

Requirement: CIP-007-6 R2.

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:

Changed to October 1, 2010

Violation Start Date: July 01, 2016

End/Expected End Date: October 28, 2016

Region Initially Determined a Violation On:

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: Prior to September 2016, the only listed patch sources for all [redacted] workstations, was [redacted] The [redacted] is generated by [redacted] only for their supported software. Historically [redacted] workstations used [redacted] as patch sources, however since the [redacted] workstation's installation, several different programs have been installed (e.g. [redacted] etc.) to support administrative work. These software packages were thought to be covered by [redacted] via their [redacted] report. After discussion with other Business Units, it was discovered that they were not covered in the [redacted] report and as such no review of patch sources was conducted.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Mitigating Activities:
1) the patch source template was reviewed by the [redacted] patching team and updated to show the correct patch source vendors, (Complete)
2) the patch sources were reviewed for applicable patches (Complete) and
3) all applicable patches were installed via change order [redacted].(Complete)

Preventative Measure: On 10/13/16, a meeting will be held to conduct a C3

session among SMEs to share current practice related to determining software patch source.

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 and Actual Impact to the BES is low. If there are any exploitable vulnerabilities the individual would at least need access to the [redacted] workstation.

Risk Assessment of Impact to BPS: [redacted] identifies that that potential impact to the BES is low. [redacted] has not experienced any negative impact 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			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
RFC2016016342	CIP-007-6 R2.	**Changed to CIP-007-3a R3**

Mitigation Plan Submitted On: [redacted]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: July 31, 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		
RFC2016016342	07/01/2016	CIP-007-6 R2.
Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.		

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

Summary of Violation
The [redacted] equipment, which was installed prior to the NERC-CIP requirements, was supplied by [redacted] However, since [redacted] installation, several different programs have been installed (e.g. [redacted] etc.) to support administrative work on multiple device types. All of the installed software were known and listed in the baseline. However, as the administrative software was not reviewed by [redacted] they were not patched. The [redacted] team did not patch administrative programs that were added after the original [redacted] software was installed. Due to the software versions found, this issue pre-dated v5/v6 implementation.

Cause of Violation
The installation of [redacted] system pre-dated NERC CIP requirement. The [redacted] team assumed that all of the programs installed on the equipment under their purview were covered by [redacted] This resulted in multiple administrative packages not being patched as a result of an incorrect patch source.

Identification Mechanism
During a Mock Audit in June 2016, the [redacted] SME was discussing their patch sources. They were in the process of removing software that was not essential to their system and not reviewed by [redacted] team members were in the audience listening to this discussion when they realized that they have some of the same software installed on several of their devices that were attributed to [redacted] as the patch source.

Scope Review (Extent of Condition)
On July 16, 2016, [redacted] discovered that [redacted] does not cover all software packages. Upon this discovery, a cursory review of all software packages was conducted to see if they were covered by [redacted]

Results of initial review: The [redacted] team reviewed the software packages installed on their assets. During the review, multiple software packages were discovered to not be covered by [redacted] Upon investigation of the primary source of these software packages, it was determined that there were several packages that had applicable patches and they were patched.

Scope Review (Extent of Condition) Update

Upon completion of this task an Effectiveness Review was scheduled and held by the [redacted] and it was determined that the Extent of Condition should be expanded to all Business Units ([redacted] that have equipment covered by NERC-CIP. Therefore, a Patch Source Review will be conducted by the [redacted] that have NERC-CIP assets. In addition, four new milestones were developed based on the work done by the [redacted] team for this Mitigation Plan to definitively determine all software patch sources and update or mitigate any vulnerabilities for patch sources identified that differ from [redacted]

Root Cause
The [redacted] equipment, which was installed prior to the NERC-CIP requirements, was supplied by [redacted] As the NERC CIP requirements went into place, [redacted] made an assumption that [redacted] covered all of the software installed on all of the equipment and this assumption was never validated. To validation this assumption, someone from the [redacted] team, with the help of the vendor, will have to review all software packages installed on all Operating Systems. The system pre-dates the NERC-CIP requirements and the

[redacted] ([redacted] process ([redacted] NERC-CIP asset change control process for new assets).

Table 1 Timeline

Date	Event
May 2008	[redacted] System Installation
May 2008 - September 2015	Administrative Software packages installed
10/20/15	[redacted] go live
7/1/16	v5 goes live
7/16/16	Identification of issue
7/16/16	Started review of Patch Source and applicable patches
7/16 - 7/29/16	All other packages and Operating System were patched during monthly patch cycle.
9/29/16	Completed review of Patch Source and applicable patches
10/10/16	Installed patches
10/24/16	Knowledge share
12/07/2016	Effectiveness Review
3/07/2017	Extent of Condition review of patch sources

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

During a Mock Audit, the [redacted] SME was discussing their patch sources. They were in the process of removing software that was not essential to their system. [redacted] team members were in the audience listening to this discussion when they realized that they have some of the same software and that it was not covered by [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:

Corrective Actions
Upon realizing that not all software was covered by [redacted] multiple members of the [redacted] Team reviewed all of the installed software packages to see which packages were covered by [redacted] For the software packages easily determined to not be covered by [redacted] the proper patch source was identified (Milestone 1). The software with a new patch source was evaluated to determine if the patch source had issued any applicable patches (Milestone 2). For the software packages that had applicable patches, they were applied via change order [redacted] (Milestone 3).
Corrective Actions update
Using the [redacted] Project, all Business Units that have NERC-CIP equipment (e.g. workstations, servers, firewalls, etc.) conducted a review of their patch source inventory and confirmed that their patch sources are inclusive of all applicable patch source information (Milestone 6). No errors were found.
The [redacted] team will split the software packages, Operating Systems, etc. into two categories: 1) software that we can conclusively prove the patch source or 2) software that we cannot conclusively prove the patch source. The expected outcome is that all software packages and Operating System will be listed on one of two lists. The first list definitively shows the patch source and the second list is an input to the next milestone. We are taking this action because by filtering out the first list, this lowers the complexity of the work in the following milestones (Milestone 7).
For the software packages that we cannot conclusively prove the patch source, with the help of [redacted] verify that the software is need. The expected outcome is that this will determine what software is required and supported by the vendor. We are taking this action because due to the age of the system and the lack of as-built documentation, vendor support is needed to establish what installed software is required and supported by the vendor (Milestone 8).
For the software that does not have a business reason, it will be removed from the asset(s). The expected outcome is that any software installed on an asset that does not have a business reason will be removed from the asset following the [redacted] process. We are taking this action because this will decrease the complexity of the baseline and subsequent path source/patch evaluation. Consequently, this will also help to lower the risk to future vulnerabilities (Milestone 9).
For the software that has a business reason but is not evaluated by the [redacted] determine the patch source. The expected outcome is that all software installed on NERC CIP equipment under the purview of [redacted] will have a verified patch source. For the software packages that have a business reason and are not evaluated by [redacted] a new patch source will have to be named and it will need to be evaluated. If any security patches have been released, they will be applied (or mitigated). We are taking this action to comply with NERC CIP007 (Milestone 10).

Preventive Actions
A C3 (lessons learned) session was conducted among SMEs representing each Business Unit to share current practice related to determining software patch source (Milestone 4).

The [redacted] is used whenever a change is made to any NERC related equipment. The purpose of the [redacted] process is to prevent duplicate work, to improve communication between business units about configuration changes within [redacted] and to consistently and correctly manage configuration changes to all BES Cyber Assets (BCAs). The process ensures the exchange of change and configuration information to verify and validate impacts created by required changes to BCAs. This process leverages the existing IT Change Order process, with oversight provided by the IT [redacted] ([redacted] which includes the [redacted] Board. The [redacted] board, which includes representatives from key business units, meets weekly to review evidence of additions/deletions/changes to BCAs as required by NERC CIP. This process applies to all [redacted] BES Cyber Systems and their associated EACMSs, PACSs, and PCAs. The [redacted] process also applies to the addition, modification, or deletion of any BCA associated with a [redacted] or [redacted] BES Cyber System (BCS). All changes that revise the baseline configuration of a BCA (including hardware or software) are covered by this process.

Detective Actions

The [redacted] Project Manager is responsible for the overall Management of the Program Activities with support from the [redacted] Directors, Managers, Supervisors and Asset Owners from the following Business Units; [redacted] and [redacted] This team collaborates to implement a consistent method of measuring and monitoring the NERC CIP [redacted] Compliance activities for all CIP Standards and Requirements. [redacted] NERC CIP Program Owners of CIP Standards & Requirements is the framework to holistically manage the [redacted] NERC CIP Program. This Program Management approach leverages a matrix management model that includes Business Unit Leadership of a Director, Manager and [redacted] Partner for each CIP Standard and Requirement. This Best in Class management approach enables the Program Leaders of each CIP Standard and Requirement to provide the guidance and expertise as required with other Business Unit Managers, Supervisors, Asset Owners and Subject Matter Experts to perform the necessary work to maintain compliance. Monthly the [redacted] Project validates the generation of CIP-007 requirements (e.g. Patch Source List, Patch Evaluations, etc.)

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: July 31, 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
Revise patch source template	The patch source template was reviewed by the [redacted] patching team and updated to show the correct patch source vendors	09/09/2016	09/29/2016		No
Evaluate patch new sources	The newly identified patches from third party (non-[redacted] sources were evaluated for applicability	09/29/2016	09/29/2016		No
Install required patches	All applicable patches were installed via change order 25392.	10/11/2016	10/02/2016		No
Knowledge sharing Session	A meeting will be held to review lessons learned (C3) among SMEs to share current practice related to determining software patch source.	10/24/2016	10/24/2016		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
Effectiveness Review	Group review of the taken mitigation activities.	12/07/2016	12/07/2016		No
Extent of Condition review of patch sources	[redacted] review of current patch sources	03/07/2017	02/28/2017		No
Software Disposition	Split the [redacted] software packages, Operating Systems, etc. into two categories	03/31/2017			No
Software Verification	Verify that the remaining software is needed	06/30/2017			No
Remove software that is not needed	Remove the unneeded software	07/14/2017			No
Determine patch source and update as necessary	For software with a business reason not covered by [redacted] identify a new patch source and update (or mitigate) as necessary.	07/31/2017			No

Additional Relevant Information

Milestone Activity Completion Date
Revise patch source 09/09/2016
Evaluate patch sources 09/29/2016
Install required patches 10/11/2016
Knowledge share 10/24/2016
Effectiveness Review 12/07/2016
Extent of Condition review of patch sources 3/07/2017
Software Disposition 3/31/2017
Software Verification 6/30/2017
Remove software that is not needed 7/14/2017
Determine patch source and update as necessary 7/31/2017

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.

While implementing this Mitigation Plan, [redacted] determines that the risk to the reliability of the BPS remains low until this Mitigation Plan is implemented. There are various compensating measures in place as part of an in-depth protection strategy. Any vulnerability in the Cyber Assets that were present due to an unpatched application was mitigated due to [redacted] layered approach to Defense-in-Depth that includes isolation by firewalls. This makes it difficult for unauthorized internal or external access to occur. The Cyber Assets are monitored for electronic and physical access; specifically access reports are generated and reviewed by the [redacted] security personnel to monitor unauthorized attempts into the electronic and physical perimeter. This allows any access to the assets to be known immediately at the time of access.

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 implementing the [redacted] for change control of NERC CIP [redacted] has a control to ensure that the reliability standard is not violated in the future. Additionally, [redacted] conducted a weekly [redacted] meeting to ensure the employees understand the requirements of the standard and what is required of each employee to meet the requirements of the standard.

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

The [redacted] group has taken the perform a systematic vulnerability assessment on the [redacted] system using tools like [redacted] patch assessment and [redacted] The software licenses have been purchased and the necessary configuration is being scheduled. Once the configuration has been completed we will be able to perform the vulnerability assessment. The results of the assessment will be reviewed and [redacted] will determine what actions, if any, can be done to minimize our vulnerabilities, while ensuring the operations of a critical [redacted] system.
Patching and vulnerability assessments will be planned and implemented immediately on the new [redacted] environments that are in process for a 2018 deployment.

In addition, [redacted] will be enhancing our vulnerability management program to move beyond the required annual active vulnerability assessment. We intend to re-structure the program to utilize vulnerability management as the initiation point for identification and management of all active vulnerabilities. Identified vulnerabilities will be tracked by asset and based on the assigned severity level (1 being critical and 5 being minimal impact) will have an appropriate mitigation plan and timeline developed. All level 1 and level 2 vulnerabilities will be required to have a mitigation plan with key tasks to mitigate the immediate security risk and be assigned for monitoring for vendor released patches. This will lead directly into our patch management program to monitor each assigned patch source for new patches. The use of the vulnerability mitigation plan outside of the patching mitigation plan will ensure that all vulnerabilities for all software is monitored and potential patches identified regardless of the specific patch source specified. By combining both approaches [redacted] will ensure that vendors are managing and ultimately correcting the critical issues that exist within their software. The program will be set to evaluate vulnerabilities on a monthly basis to ensure vulnerabilities are identified and appropriate mitigation plans put into place in a timely manner.
The first phase of this program enhancement is already in process of being implemented. [redacted]

has procured [redacted] as part of the automation of our baseline collection and monitoring which is planned for completion by the end of Q3 2017. The [redacted] module was also procured and will be installed after the primary [redacted] product is in place and operational. Even with the initial deployment of [redacted] will be able to quickly identify the current software and patches installed and via the reporting and monitoring quickly identify issues between the patch evaluation and deployed software automatically instead of by doing manual QA reviews. Once the [redacted] modules are installed, then [redacted] will be able to develop a robust vulnerability management program as described above which is planned for completion in the first half of 2018.

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): RFC2016016342
Mitigated Standard Requirement(s): CIP-007-6 R2. **Changed to CIP-007-3a R3**
Scheduled Completion as per Accepted Mitigation Plan: July 31, 2017
Date Mitigation Plan completed: July 31, 2017
RF Notified of Completion on Date: [redacted]
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2016016342 Certification Package.zip	File "RFC2016016342 Certification Package.zip" contains cover page for the package and also the supporting evidence for each milestone.	16,782,942

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 RFC2016016342

[redacted]

Standard/Requirement: CIP-007-6 R2 **Changed to CIP-007-3a R3**

NERC Mitigation Plan ID: RFCMIT012397-1

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	**Mitigation Plan Submittal**	**RF Acceptance**	**NERC Approval**	**Certification Submittal**	**Date of Completion**
Self-Report [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	07/31/17

Description of Issue

The [redacted] ([redacted] equipment, which was installed prior to the NERC-CIP requirements, was supplied by [redacted] However, since [redacted] installation, several different programs have been installed (e.g. [redacted] etc.) to support administrative work on multiple device types. All of the installed software were known and listed in the baseline. However, as the administrative software was not reviewed by [redacted] they were not patched. The [redacted] team did not patch administrative programs that were added after the original [redacted] software was installed. Due to the software versions found, this issue pre-dated v5/v6 implementation.

Evidence Reviewed		
File Name	**Description of Evidence**	**Standard/Req.**
File 1	RFC2016016342 Certification Package	CIP-007-6 R2

Verification of Mitigation Plan Completion

Milestone 1: Revise patch source template.

File 1, "*RFC2016016342 Certification Package*", Milestone 1 Evidence, Pages 3 through 33, show the affected patch source documents with the applicable changes highlighted and bookmarked. Page 2 summarizes the work order used to make the changes, showing completion on September 9, 2016.

Proposed Completion Date: September 9, 2016

Actual Completion Date: September 9, 2016

Milestone # 1 Completion verified.

Milestone 2: Evaluate patch new sources.

File 1, "*RFC2016016342 Certification Package*", Milestone 2 Evidence, Pages 3 through 78, show the identification and assessment of patches for the newly identified applications. The date of assessment is shown as September 29, 2016.

Proposed Completion Date: September 29, 2016

Actual Completion Date: September 29, 2016

Milestone # 2 Completion verified.

Milestone 3: Install required patches.

File 1, "*RFC2016016342 Certification Package*", Milestone 3 Evidence, Page 5, shows completion of patching on October 2, 2016. Pages 6 and 7, show details of the changes made to the installed software.

Proposed Completion Date: October 11, 2016

Actual Completion Date: October 2, 2016

Milestone # 3 Completion verified.

Milestone 4: Knowledge sharing session.

File 1, "*RFC2016016342 Certification Package",* Milestone 4 Evidence, Pages 2 through 8, show a slide deck used at a meeting of SMEs held on October 24, 2016. Page 9, shows the attendee sign-in for that meeting.

Proposed Completion Date: October 24, 2016

Actual Completion Date: October 24, 2016

Milestone # 4 Completion verified.

Milestone 5: Effectiveness review.

File 1, "*RFC2016016342 Certification Package",* Milestone 5 Evidence, Page 1, documents an effectiveness review held with [redacted] and RF staff at the [redacted] offices on December 7, 2016. Follow-up meetings were held with [redacted] staff as documented on Pages 3 through 8. A final follow-up with [redacted] and RF staff was held on a conference call on February 24, 2017.

Proposed Completion Date: December 7, 2016

Actual Completion Date: December 7, 2016

Milestone # 5 Completion verified.

Milestone 6: Extent of Condition review of patch sources.

File 1, "*RFC2016016342 Certification Package",* Milestone 6 Evidence. Page 2, contains attestations of completion of an extent-of-condition review by all affected [redacted] asset types, with the latest completion date of February 28, 2017. While use of attestations as evidence of work completed is considered weak, this evidence us supported by more detailed evidence in Milestone 7.

Proposed Completion Date: March 7, 2017

Actual Completion Date: September 29, 2016

Milestone # 6 Completion verified.

Milestone 7: Software disposition.

File 1, "*RFC2016016342 Certification Package",* Milestone 7 Evidence, Pages 2 and 3, show the list of software known by [redacted] not to be included in [redacted] [redacted] patch report. Pages 4 through 40, contain the list of software for each class of asset that [redacted] is unsure of. [redacted] states that this list was submitted to [redacted] for review. [redacted] response is evidenced in Milestone 8. No date is included in these reports. However, File 1, "*RFC2016016342 Certification Package",* Milestone 8 Evidence Page 2, shows opening of a case with [redacted] support on March 7, 2017 with this information.

Proposed Completion Date: March 31, 2017

Actual Completion Date: March 7, 2017

Milestone # 7 Completion verified.

Milestone 8: Software verification.

File 1, "*RFC2016016342 Certification Package",* Milestone 8 Evidence, Pages 2 through 5, show a ticket opened with [redacted] support to identify information about the packages that were listed as "unknown" in Milestone 7. Pages 43 through 125, show [redacted] evaluation of [redacted] response to the questions about whether the software was needed and if so, was it included in [redacted] [redacted]

patch summary. No dates are included in the evidence. However, File 1, "*RFC2016016342 Certification Package",* Page 4, of Milestone 9 Evidence shows initiation of a work order to remove software identified by this process as not needed on July 5, 2017.

Proposed Completion Date: June 30, 2017

Actual Completion Date: July 5, 2017

Milestone # 8 Completion verified.

Milestone 9: Remove software that is not needed.

File 1, "*RFC2016016342 Certification Package",* Milestone 9 Evidence, Pages 3 and 4, show a ticket created to remove software identified as not needed. That software is listed on Page 3. PDF Pages 6 through 1157, show a baseline taken after package removal. Examination of a small sample of software shows that the software in the list was removed. Page 6, shows the baseline date of July 24, 2017.

Proposed Completion Date: July 14, 2017

Actual Completion Date: July 24, 2017

Milestone # 9 Completion verified.

Milestone 10: Determine patch source and update as necessary.

File 1, "*RFC2016016342 Certification Package",* Milestone 10 Evidence, Pages 2 through 554, shows a detailed patch source listing for each applicable system. This patch list shows changes identified by the process in Milestones 7-9. For example, a patch source list from October 2016 shows [redacted] software as having [redacted] as a patch source whereas the list provided for this Milestone shows [redacted] as the patch source. No date is provided in the PDF. However, the PDF itself shows a creation date of July 31, 2017.

Proposed Completion Date: July 31, 2017

Actual Completion Date: July 31, 2017

Milestone # 10 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: [redacted]

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation