

Attachment 9

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

- 9.a The Entity's Self-Report (RFC2016016343);
- 9.b The Entity's Self-Report (RFC2016016343) submitted [REDACTED];
- 9.c The Entity's Mitigation Plan designated as RFCMIT012609 submitted [REDACTED];
- 9.d The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
- 9.e ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
- 9.f The Entity's Self-Report (RFC2017017777);
- 9.g The Entity's Mitigation Plan designated as RFCMIT013020 submitted [REDACTED];
- 9.h The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
- 9.i ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
- 9.j The Entity's Self-Report (RFC2017017839);
- 9.k The Entity's Mitigation Plan designated as RFCMIT013016 submitted [REDACTED];
- 9.l The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
- 9.m ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
- 9.n The Entity's Self-Report (RFC2018020386);
- 9.o ReliabilityFirst's Verification of Mitigating Activities Completion dated [REDACTED]

Self Report

Entity Name: [REDACTED] ([REDACTED])

NERC ID: [REDACTED]

Standard: CIP-007-6

Requirement: CIP-007-6 R2.

Date Submitted: [REDACTED]

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED] [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: July 01, 2016 **Changed to August 26, 2016**

End/Expected End Date:

Region Initially Determined a August 25, 2016

Violation On:

Reliability Functions: [REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]

Is Possible Violation still No
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: [REDACTED] report (source for [REDACTED] system) was issued on 7/1/2016 and the evaluation was conducted on 07/21/2016. In the evaluation is patch

[REDACTED] The evaluation states that the patch will not be applied because it will "break" the application. As such, mitigation plan [REDACTED] will be revised to include this patch. The mitigation plan was updated on 09/23/2016 that is beyond 35 days as required by the standard.

Mitigating Activities:

Description of Mitigating
Activities and Preventative
Measure:

Mitigating Activities: We are running [REDACTED] on new [REDACTED] hardware. [REDACTED] hardware is running [REDACTED]; [REDACTED]. There are a number of [REDACTED] that have been identified in our patching spreadsheets. For the [REDACTED] is what is required for [REDACTED]. Our Vendor, [REDACTED] has said we should not install anything above [REDACTED] and [REDACTED] on our servers because it will impact [REDACTED]. [REDACTED] has end of life'd (EOL) the [REDACTED] application and will not be producing any enhancements to the product. Ultimately, it will be resolved with the installation of new [REDACTED] system in

Self Report

December, 2018.

In addition, the following compensating measures to mitigate risk exposure are: 1) The protection provided by firewalls configured to specifically limit connections to our corporate network via a [REDACTED] and deny communications to / from the internet 2) We run [REDACTED] scans and ports and services scans to validate defined cyber security controls. We run these scans once a month and 3) Implementing [REDACTED] to restrict access of [REDACTED] to only the static [REDACTED] of the documented users on the system. This solution will prevent any adversary from executing remote code or exploiting any [REDACTED] vulnerability.

Preventative Measure: The following four actions are taken to prevent this event from occurring again: 1) The patch SWI will be revised to include a checklist, 2) The [REDACTED] Patch Evaluation (2.2) and Deployment (2.3)" template will be revised to include a column "Existing or New Mitigation Plan?", 3) Mitigation Plan template will be revised to include a section on revisions and 4) Share process improvements (C3 event) with other [REDACTED]

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Moderate

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to the BES is low. While the mitigation plan was not updated, the vulnerability of not updating [REDACTED] was already evaluated and compensating measures have already been established.

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			

Self Report

Entity Name: [REDACTED] ([REDACTED])

NERC ID: [REDACTED]

Standard: CIP-007-6

Requirement: CIP-007-6 R2.

Date Submitted: [REDACTED]

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED] [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: October 31, 2016

End/Expected End Date: December 06, 2016

Region Initially Determined a
Violation On:

Changed to August 26, 2016-Based on the entity's evaluation of the patches (7-21-2016), it had to apply the patches on or before 8-25-16. The violation started the next day when they failed to do so.

Reliability Functions: [REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]

Is Possible Violation still No
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: The [REDACTED] has an individual that evaluates patches and another individual that applies the patches specified in the evaluation. The evaluations are divided by Operating System (e.g. [REDACTED] etc.). The [REDACTED] patches are assessed for applicability and then a decision is made wither or not to apply them. If the patch applies to all [REDACTED] machines, the row is highlighted. In the July evaluation, two [REDACTED] patches were assessed to be applied only to 5 [REDACTED] systems, but the installation did not happen. Because these two patches did not apply to all [REDACTED] machines the rows were not highlighted. Instead the last two columns were highlighted to signify that they needed to be applied. Once the evaluation was complete, the list was informally left with the individual that was to install the patches. This person installed all of the patches whose row was highlighted in yellow, missing the two patches.

Patch Description:

[REDACTED]
[REDACTED]
[REDACTED] It contains the following
metrics:

[REDACTED]
[REDACTED]

Self Report

[REDACTED]

The timeline of events was as follows:
7/1/2016 [REDACTED] report was released
7/21/2016 Patches were evaluated
7/21/2016 [REDACTED]
8/21/2016 [REDACTED]
8/21/2016 [REDACTED]
8/25/2016 35 Day Window Ends
10/5/2016 Issue identification
10/6/2016 Patches were applied via [REDACTED]

Mitigating Activities:

Description of Mitigating Activities: 1) The two patches were applied to the [REDACTED] systems within 24 hours of the identification of the gap.
Preventative Measure:

Preventative Measures: 1) Previously, all evaluated patches were sorted by OS manufacture (Such as [REDACTED] etc...). From now on, all patches will be sorted by OS type (Such as [REDACTED] etc..), 2) Process Map will be revised to incorporate the pre-job brief requirement and 3) the patching SMEs will discuss the lessons learned at a C3 session (10/20/2016).

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe
Actual Impact to BPS: Minimal

Self Report

Description of Potential and Actual Impact to BPS: As per the VSL the impact could be severe. However, given that 2 patches were missed only on [REDACTED] systems. Those [REDACTED] systems were up-to-date with patches up to that point. Our internal processes discovered it and the systems were patches within 24 hours of the identification of the problem. The two patches described above were missed on [REDACTED] computers. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Hence, the Potential and Actual Impact to the BES is low. Hence, the Potential and Actual Impact to the BES is low.

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: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2016016343	CIP-007-6 R2.	

Mitigation Plan Submitted On: [REDACTED]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: February 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		
RFC2016016343	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:

Violation #1

A [redacted] team member completed the review of [redacted] report and it was determined that patch [redacted] was not to be applied because it will "break" the application. Therefore, the patch was to be added to the existing patch mitigation plan that covers the [redacted] vulnerability [redacted]. However, the patch mitigation plan was not updated in the required 35-day window.

Violation #2

A [redacted] team member completed the review of [redacted] report and it was determined that there were two [redacted] patches ([redacted]) that applied to only [redacted] machines that are a part of the [redacted]. It was determined that these two patches were to be applied; but the application did not happen within the required 35-day window.

Cause of Violations

The cause for both violations is due to the intensive manual process that led to a human performance error in hand off between the [redacted] employees.

Identification Mechanism

Our internal QA program identified both violations.

Root Cause

[redacted] reviews all of the software vendors (e.g. [redacted] for software that they have installed on their systems. Then they review the patches for applicability and functionally test the applicable patches. This is used to generate the [redacted] Report which is issued quarterly. It was assumed by the [redacted] team that the [redacted] Report covered all software installed. [redacted] report is the identified patch source for the [redacted] equipment.

The [redacted] has an individual that evaluates patches and another individual that applies the patches specified in the evaluation. The evaluations are divided by Operating System (e.g. [redacted] etc.). The patches are assessed for applicability and then a decision is made whether or not to apply them. Next the evaluation is handed off to another individual to complete all required work.

Violation #1

Specifically, at the completion of the [redacted] evaluation, it was determined that patch [redacted] was not to be applied because it will "break" the application. There is a mitigation plan [redacted] open against the [redacted] vulnerability and it was determined that it was to be updated to include the new patch. However, the mitigation plan was not updated in the required 35-day window. This was due to the Patch Mitigation Plans not being formally tracked.

Violation #2

Included in the evaluation of all applicable [redacted] patches were two [redacted] patches ([redacted]). They were assessed and it was determined that they only applied to [redacted] systems and that they were to be applied; but the application did not happen. If the patch applies to all [redacted] machines, the evaluator highlights the row in the evaluation Excel workbook. Because these two patches did not apply to all [redacted] machines, the evaluator did not highlight the row for each of these

patches. Instead, the evaluator highlighted the last two columns to signify that they needed to be applied only on the two [REDACTED] machines. After the evaluation was complete, the list was informally left with the individual that was to apply the patches. The person applying the patches looked for rows (and applied the patches) that were highlighted in yellow and missed the two patches. Intensive manual process led the error in hand off between evaluator and the person who applies the patches.

Date Action	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED] 1/2016 [REDACTED] [REDACTED] report was released		X	X
7/21/2016 Patches were evaluated	X		X
7/21/2016 [REDACTED]			X
8/21/2016 [REDACTED]			X
8/21/2016 [REDACTED]			X
8/25/2016 35 Day Window Ends	X		X
9/22/2016 Issue identification - Mitigation Plan not updated		X	
9/23/2016 Mitigation Plan updated		X	
10/5/2016 Issue identification - Patches not installed			X
10/6/2016 Patches were applied via [REDACTED]			X

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

Scope Review (Extent of Condition)

Violation #1

Of the four patches evaluated in the July evaluation, it was determined that only one patch would break the application, the other patches were applied.

Violation #2

The August Baseline was reviewed to confirm that all Patches Evaluated in the July assessment were applied.

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

Violation #1

In addition, the Patching Mitigation Plan [REDACTED] will be revised to include [REDACTED] (Milestone 1).

Violation #2

The two patches were applied to the [REDACTED] systems the day after the issue identification via Change Order [REDACTED] (Milestone 2).

Preventive Actions

Violation #1

The following actions are to be taken to prevent this event from occurring again: a process change rapid experiment will be conducted. In this experiment, a formal handoff between evaluation and application via a pre-job brief will be used instead of the current method (Milestone 4), upon successful completion of the experiment, [REDACTED] Patch Management Process Map will be revised (Milestone 6), the Mitigation Template will be revised to add a section for revisions (Milestone 7) and a lessons learned (C3 event) to share these events with Business Unit representatives so that the lessons learned can be disseminated to all Business Units (Milestone 5). 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 High- or [REDACTED] [REDACTED] BES Cyber System (BCS). All changes that revise the baseline configuration of a BCA (including hardware or software) are covered by this process.

Violation #2

The [REDACTED] will be revised to include the need for a task to be added to the change order when a Mitigation Plan needs to be created/revised (Milestone 8) and this change will be disseminated to the SMEs (Milestone 9).
The IBCUR process (see above).

Detective Actions

Violation #1

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] [REDACTED] [REDACTED] [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]

Violation #2

Previously, all evaluated patches were sorted by OS manufacture (Such as ██████████ etc...). From now on, all patches will be sorted by OS type (Such as ██████████ ██████████ ██████████ etc.). In addition, the newly revised Patch Template will be used (Milestone 3).

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: February 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
Update Mitigation Plan	Update Mitigation Plan to include ██████████ 11.31 ██████████ ██████████ ██████████ ██████████	09/23/2016	09/23/2016		No
Apply ██████████ patches	Apply missed patches to ██████████ systems	10/06/2016	10/06/2016		No
New patch evaluation template	Use of new patch evaluation template	10/07/2016	10/31/2016		No
Process change rapid experiment	Rapid experiment of a formal handoff between evaluation and application via a pre-job brief	10/11/2016	10/24/2016		No
Knowledge share	A meeting will be held to review lessons learned (C3) among representative SMEs to share current practice related to determining software patch source.	10/20/2016	10/24/2016		No
Revise ██████████ Patch Management Process Map	Process map revision to include the pre-job brief requirement	10/21/2016	10/24/2016		No
Revise patch mitigation plan template	Revise patch mitigation plan template to include a section on revisions	01/13/2017	12/19/2016		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
Revise [REDACTED]	Revise [REDACTED] to include the need for a task to be added to the change order when a Mitigation Plan needs to be created/revised.	02/03/2017			No
Disseminate changes [REDACTED]	A meeting will be held among SMEs to share to the changes to the Mitigation plan and [REDACTED] process.	02/10/2017			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.

For both violations, while implementing this Mitigation Plan [REDACTED] determines that the risk to the reliability of the BPS remains low until this Mitigation Plan is implemented.

Violation #1

The following compensating measures were implemented (per "[REDACTED] MitPlan-001") to mitigate risk exposure: 1) The protection provided by firewalls configured to specifically limit connections to our corporate network via a [REDACTED] and deny communications to / from the internet 2) We run [REDACTED] scans and ports and services scans to validate defined cyber security controls; these scans once a month and 3) Implementing [REDACTED] [REDACTED]) to restrict access of [REDACTED] to only the static [REDACTED] of the documented users on the system. This solution will prevent any adversary from executing remote code or exploiting any [REDACTED] vulnerability.

Violation #2

For the missed [REDACTED] patches, per the VSL the impact could be severe. However, given that 2 patches were missed only on [REDACTED] systems. Those [REDACTED] systems were up-to-date with patches up to that point. Our internal processes discovered it and the systems were patched within 24 hours of the identification of the problem. The two patches described above were missed on [REDACTED] computers.

[REDACTED]

[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

Both issues were caused by a gap in the process during the hand off between the patch evaluator and either the person who applies the patches ([REDACTED] or, the person who writes the mitigation plan ([REDACTED] The relevant guidance documents and process diagrams have been identified and will be revised. This will increase communication between both parties, minimizing the probability that these types of events will occur again.

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



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): RFC2016016343

Mitigated Standard Requirement(s): CIP-007-6 R2.

Scheduled Completion as per Accepted Mitigation Plan: February 17, 2017

Date Mitigation Plan completed: February 21, 2017

RF Notified of Completion on Date: [REDACTED]

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2016016343 Certification Package.zip	File RFC2016016343 Certification Package.ZIP contains the coverage and supporting evidence for each milestone.	6,735,988

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 RFC2016016343

██████████

Standard/Requirement: CIP-007-6 R2

NERC Mitigation Plan ID: RFCMIT012609

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	Mitigation Plan Submittal	RF Acceptance	NERC Approval	Certification Submittal	Date of Completion
Self-Report ██████████	██████████	██████████		██████████	02/21/17

Description of Issue

Violation #1: A ██████████ team member completed the review of ██████████ report and it was determined that patch ██████████ was not to be applied because it would "break" the application. Therefore, the patch was to be added to the existing patch mitigation plan that covers the vulnerability ██████████. However, the patch mitigation plan was not updated in the required 35-day window.

Violation #2: An ██████ team member completed the review of ██████████ report and it was determined that there were two '██████████' patches (██████████) that applied to only ██████ machines that are a part of the ██████████ (██████). It was determined that these two patches were to be applied; but the application did not happen within the required 35-day window.

The cause for both violations is due to the intensive manual process that led to a human performance error in hand off between the ██████ employees.

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	Milestone 1- Submit	CIP-007-6 R2
File 2	Milestone 2- Submit	CIP-007-6 R2
File 3	Milestone 3- Submit	CIP-007-6 R2
File 4	Milestone 4- Submit	CIP-007-6 R2
File 5	Milestone 5- Submit	CIP-007-6 R2
File 6	Milestone 6- Submit	CIP-007-6 R2
File 7	Milestone 7- Submit	CIP-007-6 R2
File 8	Milestone 8- Submit	CIP-007-6 R2
File 9	Milestone 9- Submit	CIP-007-6 R2
File 10	RFC2016016343 Certification Cover Page	CIP-007-6 R2
File 11	RFC2016016343 [REDACTED] Patch	CIP-007-6 R2

Verification of Mitigation Plan Completion

Milestone 1: Update Mitigation Plan.

File 1, “*Milestone 1 – Submit*”, document Page 2, dated September 23, 2016, shows the Vendor, Asset numbers, and the Patch numbers. Page 5 shows the listed patch that could not be applied to the [REDACTED] servers. It was additionally signed and change noted on Page 7, with SME signatures. Pages 10 through 12 include a spreadsheet showing the IT patch evaluation with the listed patch and the applicable system [REDACTED] system names and their current version.

The Mitigation Plan's compensating measures did not change as the [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Milestone # 1 Completion verified.

Milestone 2: Apply [REDACTED] patches.

File 11, “*RFC2016016343 LMV Patch*”, is a screenshot of a [REDACTED] [REDACTED] [REDACTED] showing the two patches that were installed on the [REDACTED] Machines.

Milestone # 2 Completion verified.

Milestone 3: New patch evaluation template.

File 3, “*Milestone 3 – Submit*”, shows the new evaluation template. Page 2 shows the previous evaluation template, noting that it is not very clear what system or device the patch applies to. Page 12 shows the Cyber Asset Name, the Operating System, Software, or Firmware version and name, whether it is a patch or a vulnerability, and the patch/vulnerability ID. It also lists out each Cyber Asset that the patch applies to.

Milestone # 3 Completion verified.

Milestone 4: Process change rapid experiment.

File 4, “*Milestone 4 – Submit*”, shows an [REDACTED] Support Pre-Job Brief being used for the November 2016 patch review cycle showing a formal hand-off of the review of the patches to the person performing the patches and documenting what patches will be applied and what patches were applied back in October. This briefing is being done in person and documents the results of the briefing ensuring that the individuals who are installing the patches after the patch review process have the information and tools needed to complete the patching process.

Milestone # 4 Completion verified.

Milestone 5: Knowledge share.

File 5, “*Milestone 5 – Submit*”, document shows that a presentation was given to SMEs to discuss lessons learned from the two [REDACTED] patches. Page 9 shows a list of personnel that attended the lessons learned documenting people from [REDACTED] [REDACTED] [REDACTED] and [REDACTED]

Milestone # 5 Completion verified.

Milestone 6: Revise [REDACTED] Patch Management Process Map.

File 6, “*Milestone 6 – Submit*”, shows the added step of a pre-job briefing within the patch management process flow chart on page 2.

Milestone # 6 Completion verified.

Milestone 7: Revise patch mitigation plan template.

File 7, “*Milestone 7 – Submit*”, shows the new Patch Mitigation Plan template has changed to show the last revisions to the Mitigation Plan as documented on page 7 showing the Change Tracking section. This is to be used for situations where a new patch comes in for a BES Cyber System that already has a mitigation to remediate the vulnerability. This helps track the patches that are covered by the mitigation. A sample of the new template is on Page 13, with a revision history of the actual template on Page 19.

Milestone # 7 Completion verified.

Milestone 8: Revise [REDACTED]

File 8, “*Milestone 8 – Submit*”, document shows the changes that were made to the [REDACTED] ([REDACTED] [REDACTED]). This process and checklist ensure that there is a formal communication and hand-off between different business units and oversight of the different requirements for NERC CIP. It is noted that changes were made to the “Adding a BES Cyber System or BES Cyber Asset and Modifying a BES Cyber System or BES Cyber Asset checklists” as documented on page 17, 36, 43, and revisions documented in the revisions history on Page 53. It requires opening a new change order, task, or to open a new patch mitigation plan.

Milestone # 8 Completion verified.

Milestone 9: Disseminate [REDACTED] changes.

File 9, “*Milestone 9 – Submit*”, shows the initial meeting notification and invitation on Page 2 and 3. Pages 4 through 6 show the presentation. Page 7 shows the list of attendees.

Milestone # 9 Completion verified.

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

The Mitigation Plan is hereby verified complete.

Date: [REDACTED]

A handwritten signature in black ink, appearing to read "Tony Purgar". The signature is written in a cursive, flowing style with large loops.

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [REDACTED] ([REDACTED])

NERC ID: [REDACTED]

Standard: CIP-007-6

Requirement: CIP-007-6 R2.

Date Submitted: [REDACTED]

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED] [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: June 14, 2017 **Changed to May 5, 2017**

End/Expected End Date:

Reliability Functions: [REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]

Is Possible Violation still No
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: On May 08, 2017, while conducting the BES Cyber Assets (BCA) information validation activity of the [REDACTED] ([REDACTED]) baseline update process, the [REDACTED] Business Unit ([REDACTED]) representative for [REDACTED] discovered that [REDACTED] client software updates for [REDACTED] BCAs were not deployed as indicated in the March 30, 2017, NERC-CIP [REDACTED] [REDACTED] and the associated change order which was completed on April 28, 29017. Also, no mitigation plan was created/updated within 35 calendar days of the security patch evaluation. Further investigation by the [REDACTED] representative for [REDACTED] determined that applicable security patches were not deployed and no mitigation plan was created/updated within 35 calendar days of the security patch evaluation resulting in possible non-compliance (PNC) with CIP-007-6 R2.2. On May 08, 2017, upon discovery of the PNC, the [REDACTED] representative submitted a NERC Potential Violation Notification to [REDACTED]

Root Cause of Possible Violation:

On May 24, 2017 an [REDACTED] ([REDACTED]) was conducted to establish the PNC timeline, develop the problem description and determine the root cause(s). The causes for the PNC were determined to be an internal process failure and human performance failures.

Internal Process failure: There is a step at the 25-day mark of the [REDACTED]

Self Report

patch management process where an escalation should occur if scheduled patch deployments are not able to be completed. The escalation involves notifying the [REDACTED] representative for [REDACTED] who will then create/update a mitigation plan. The [REDACTED] representative was not notified and there is no automated triggering event in place.

Human Performance failures: [REDACTED] Asset SME did not deploy security software updates for [REDACTED] BCAs as indicated in the security patch evaluation template and associated change order. When the PNC was discovered, no effort was made to create/update a mitigation plan.

How was the violation discovered? The PNC was discovered on May 08, 2017 by the [REDACTED] representative while collecting and reviewing evidence to update [REDACTED] baselines. The [REDACTED] representative submitted a NERC Potential Violation Notification to [REDACTED] on May 08, 2017.

Timeline:

March 30, 2017: NERC-CIP BCA Patching Assessment completed.

April 28, 2017: Documented completion date for associated security patch deployment.

May 08, 2017: [REDACTED] representative discovery that security patches were not deployed on [REDACTED] BCAs and no mitigation plan was created/updated within 35 calendar days of the security patch evaluation.

May 08, 2017: [REDACTED] representative submits NERC Potential Violation Notification to [REDACTED]

May 24, 2017: [REDACTED] was conducted

May 24, 2017: Change Order initiated to deploy [REDACTED] client software updates to the [REDACTED] BCAs.

May 25, 2017: Deployment of [REDACTED] client software updates to [REDACTED] BCAs successfully completed.

Mitigating Activities:

Description of Mitigating Activities:

Activities and Preventative Measure: A change order was initiated on May 24, 2017 to deploy the [REDACTED] client software updates to the [REDACTED] BCAs. Deployment of the security patch was completed successfully on May 25, 2017.

Preventive Measures:

In 2017, [REDACTED] will be implementing a new [REDACTED] capability that will integrate with its existing [REDACTED]. This [REDACTED] capability includes change process workflows and a user interface for creating, assigning, monitoring, notification and reporting the status of change assessments, approvals, and implementation tasks. To address the internal process failure, a mitigation plan milestone activity will include investigating the use of [REDACTED] workflows to act as automated escalation and triggering controls within the patch management process.

To address the human performance failure, a mitigation plan milestone activity will include leveraging off of other [REDACTED] efforts to automate the process used to verify listed patches have successfully installed.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Moderate

Actual Impact to BPS: Moderate

The potential and actual impacts to the BPS are considered to be moderate. [REDACTED] has a documented process for evaluating cyber security patches but, in

Self Report

Description of Potential and order to mitigate the vulnerabilities exposed by applicable security patches, did
Actual Impact to BPS: not apply the applicable patches until 56 calendar days after completion of the
evaluation.

Risk Assessment of Impact to BPS: The risk of Impact to the BPS has been identified as low. The [redacted] BCAs were
being protected by a previous version of [redacted] client
software prior to the update. The software update [redacted]
• [redacted]
[redacted]
[redacted]
[redacted]

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
RFC2017017777	CIP-007-6 R2.	

Mitigation Plan Submitted On: [REDACTED]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: December 07, 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		
RFC2017017777	06/14/2017	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:

Brief Description: (What happened?)

On May 08, 2017, while conducting the BES Cyber Assets (BCA) information validation activity of the [REDACTED] baseline update process, the [REDACTED] Business Unit ([REDACTED] representative for [REDACTED] discovered that [REDACTED] client software updates for [REDACTED] BCAs were not deployed as indicated in the March 30, 2017 NERC-CIP BCA Patching [REDACTED] and the associated change order which was completed on April 28, 2017. Further investigation by the [REDACTED] representative for [REDACTED] revealed that no mitigation plan was created/ updated within 35 calendar days of the security patch evaluation. These two findings result in a possible non-compliance (PNC) with CIP-007-6 R2.3.

On May 08, 2017, upon discovery of the PNC, the [REDACTED] representative submitted a NERC PNC Notification to [REDACTED]

A change order was initiated on May 24, 2017 to deploy the [REDACTED] client software updates to the [REDACTED] BCAs. Deployment of the security patch was completed successfully on May 25, 2017.

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

On May 24, 2017 an [REDACTED] [REDACTED] was conducted to establish the PNC timeline, identify the problems that occurred and determine causes. The causes for the PNC were determined to be an internal process failure and a human performance failure.

Internal Process failure: There is a step at the 25-day mark of the [REDACTED] patch management process where an escalation should occur if scheduled patch deployments are not able to be completed within 35 days of evaluation completion. The escalation involves the [REDACTED] Asset Subject Matter Expert (SME) notifying the [REDACTED] representative for [REDACTED] who will then create/update a mitigation plan. The [REDACTED] representative was not notified. Automated triggering and escalation controls do not exist.

Human Performance failures: [REDACTED] Asset SME did not deploy security software updates for [REDACTED] BCAs as indicated in the security patch evaluation template and associated change order. When the PNC was discovered, no effort was made to create/update a mitigation plan.

After the initial self-report was filed on June 14, 2017, a follow-up [REDACTED] was conducted on July 5, 2017 to discuss the PNC extent of condition and determine root causes. Detailed review of the patch management process and process outputs (evidence) followed by a cause and effect analysis revealed that the scanning tool used to satisfy the process activity "rescan all assets after deployment of patches to confirm successful installation" only covered [REDACTED] percent of the population of [REDACTED] assets. Although only [REDACTED] of the [REDACTED] asset types at [REDACTED] not covered by the scanning tool have in the past required patching, the capability to validate successful patch deployment does not exist for [REDACTED] percent of [REDACTED] assets.

Problem Statement: Applicable security patches for [REDACTED] assets were not deployed and no mitigation plan was created/updated within 35 calendar days of the security patch evaluation.

Root Cause: The scanning tool utilized to validate successful installation of patches only covers [REDACTED] percent of the population of assets. The capability to validate successful patch deployment does not currently exist for [REDACTED] percent of [REDACTED] BCAs creating a high probability of PNC with CIP-007-6 R2.3.

Timeline:

March 30, 2017: NERC-CIP BCA Patching Assessment completed.

April 28, 2017: Documented completion date for associated security patch deployment.

May 08, 2017: [REDACTED] representative discovery that security patches were not deployed on [REDACTED] BCAs and no mitigation plan was created/updated within 35 calendar days of the security patch evaluation.

May 08, 2017: [REDACTED] representative submits NERC Potential Violation Notification to [REDACTED]

May 24, 2017: [REDACTED] was conducted to establish the PNC timeline, identify the problems that occurred and determine causes.

May 24, 2017: Change Order initiated to deploy [REDACTED] client software updates to the [REDACTED]

May 25, 2017: Deployment of [REDACTED] client software updates to 45 [REDACTED] BCAs successfully completed.

June 14, 2017: Self-Report submitted.

July 5, 2017: Follow-up [REDACTED] conducted to determine the extent of condition and root cause.

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

The PNC was discovered on May 08, 2017 by the [REDACTED] representative while collecting and reviewing evidence to update [REDACTED] baselines. The [REDACTED] representative submitted a NERC PNC Notification to [REDACTED] on May 08, 2017.

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 change order was initiated on May 24, 2017 to deploy the [REDACTED] client software updates to the [REDACTED] [REDACTED] (Milestone 1). Deployment of the security patch was completed successfully on May 25, 2017.

Preventive Actions:

- In the third quarter of 2017, [REDACTED] will be implementing a new Service Management (SM) capability to replace the existing configuration management tool and integrate with the existing Enterprise [REDACTED] platform. To address the current ad hoc 25-day trigger/escalation methods used in the [REDACTED] patch management process, [REDACTED] will work with the SM implementation team to determine if a workflow can be created/configured to act as automated escalation and triggering controls within the [REDACTED] process (Milestone 2).
- Develop a [REDACTED] Configuration Change Management - Patch Deployment Verification checklist (Milestone 3) that aligns with the NERC-CIP BCA Patching [REDACTED] utilized in the [REDACTED] and covers all [REDACTED] asset types. The intent of the Patch Deployment Verification checklist is to ensure that all scheduled patches are installed for [REDACTED] BCAs on a monthly basis.
- To address the [REDACTED] percent of assets not covered by [REDACTED] patch deployment validation scanning tool, [REDACTED] is collaborating with another [REDACTED] to leverage off their use of a scripting tool used to generate a Patch Deviation Report from existing baseline data (Milestone 4). The scripting tool will be tailored to run against [REDACTED] baseline data for each asset type immediately following a patch deployment. The deviation report will act as a preventive control to validate patches have been successfully deployed within 35 calendar days of evaluation completion.
- In the fourth quarter of 2017, [REDACTED] will be implemented to detect when patches are implemented and record the information for later review and analysis. As a preventive control to ensure applicable patches are deployed within 35 calendar days of the evaluation completion, the [REDACTED] feature of [REDACTED] will be utilized (Milestone 5) to scan local systems, harvest information and organizes it into a list, compare the information against the appropriate whitelist, and build a report based on the results. If a match is found, the report will include software package name/version and fields associated with the entry in the whitelist. If no match is found, the report will include an exception and an alert will show up in the [REDACTED] [REDACTED] dashboard.

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

Proposed Completion date of Mitigation Plan: December 07, 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 - Deploy the [REDACTED] client software	Deploy the [REDACTED] client software updates to the [REDACTED] BCAs	05/25/2017	05/25/2017		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
Milestone 2 - [REDACTED] implementation	Research the workflow capabilities within [REDACTED] to determine if a workflow can be created/configured to act as automated escalation and triggering controls within the patch management process	07/28/2017			No
Milestone 3 - Patch Deployment Verification checklist	Develop a [REDACTED] Patch Deployment Verification checklist	08/18/2017			No
Milestone 4 - Scripting tool for [REDACTED] use	Tailor existing [REDACTED] scripting tool for [REDACTED] use to generate a Patch Deviation Report from existing [REDACTED] baseline data	09/29/2017			No
Milestone 5 - [REDACTED]	Utilize the [REDACTED] feature of [REDACTED] for patch deployment verification	12/07/2017			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 [REDACTED] non-compliant BCAs at [REDACTED] were updated to the latest version of [REDACTED] client software version [REDACTED], which includes the following:

[REDACTED]

Due to the protections provided by the previous version of [REDACTED] [REDACTED] did not identify any risk or potential impacts, nor does [REDACTED] anticipate any increased risk to the reliability of the bulk power system.

Prevention

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

Successful completion of the Mitigation Plan as laid out in Section D will provide the capability to validate successful patch deployment for 100 percent of [REDACTED] BCAs as well as provide automated triggering and escalation controls to initiate creating/updating mitigation plans within 35 calendar days of the evaluation completion.

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] application will be able to assist in the automation of baseline collection for the majority of [REDACTED] devices (approximately [REDACTED]), but some devices will still need to be manually collected. Discussions are taking place with the [REDACTED] implementation team to incorporate into [REDACTED] the scripts generated in Milestone 4 to mitigate manual collection of baseline data.

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.

██████████ 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: ██████ ██████
Title: ██
Authorized On: ██████████

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): RFC2017017777

Mitigated Standard Requirement(s): CIP-007-6 R2.

Scheduled Completion as per Accepted Mitigation Plan: December 07, 2017

Date Mitigation Plan completed: December 01, 2017

RF Notified of Completion on Date: [REDACTED]

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017777 Certification Package.zip	File "RFC2017017777 Certification Package.zip" contains the cover page for the package and also supporting document for each milestone.	2,523,055

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 RFC2017017777

██████████ ██████████

Standard/Requirement: CIP-007-6 R2

NERC Mitigation Plan ID: RFCMIT013020

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

Description of Issue

On May 08, 2017, while conducting the BES Cyber Assets (BCA) information validation activity of the ██████████ (██████████ baseline update process, the ██████████ ██████████ Business Unit (██████████ representative for ██████████ discovered that ██████████ client software updates for ██████████ were not deployed as indicated in the March 30, 2017 NERC-CIP BCA Patching ██████████ and the associated change order which was completed on April 28, 29017. Further investigation by the ██████████ representative for ██████████ revealed that no mitigation plan was created/updated within 35 calendar days of the security patch evaluation. These two findings result in a possible non-compliance (PNC) with CIP-007-6 R2.3.

The causes were determined to be an internal process failure and a human performance failure.

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	RFC2017017777 Certification Package	CIP-007-6 R2

Verification of Mitigation Plan Completion

Milestone 1: Deploy the [REDACTED] client software.

Proposed Completion Date: May 25, 2017

Actual Completion Date: May 25, 2017

File 1, “RFC2017017777 Certification Package”, Milestone 1 Submit.

Narrative of Evidentiary Documentation:

File 1, “RFC2017017777 Certification Package”, Milestone 1 Submit. Evidentiary Document RFC2017017777_Milestone 1-100: Change Order [REDACTED] shows the required approvals on page 2 of 5 (sequence # 100, 200, 250 and 650) and completion of [REDACTED] client software deployment on 05/25/2017 (sequence #600). Note: Sequence 650 “[REDACTED] Approvers” indicates review/verification of required change management evidence by the [REDACTED] [REDACTED].

File 1, “RFC2017017777 Certification Package”, Milestone 1 Submit. Evidentiary Document RFC2017017777 Milestone 1-200: [REDACTED] Configuration Management Baseline document provides the 05/30/2017 updated baseline which reflects the approved (Milestone 1-100) and completed upgrade of [REDACTED] client software (see bookmarks section for Milestone 1-200). Note: Upon further review, three [REDACTED] (see bookmark [REDACTED] [REDACTED] under Milestone 1-200) had mitigation plans in place (see RFC2017017777_Milestone 1-300).

File 1, “RFC2017017777 Certification Package”, Milestone 1 Submit. Evidentiary Document RFC2017017777 Milestone 1-300: Mitigation Plan List. The mitigation plan list is maintained through the [REDACTED] and was filtered to show the [REDACTED] [REDACTED] assets with mitigation plans in place.

File 1, “RFC2017017777 Certification Package”, Milestone 1 Submit. Evidentiary Document RFC2017017777 Milestone 1-400: Change Order [REDACTED] documentation showing actions taken to decommission [REDACTED] (the noted asset in the description section that was decommissioned). The [REDACTED] was taken out of service on 12/01/2017. Change Order tasking is still pending to remove the asset from the BCS Asset List.

Milestone 1-100 (Page 3)

Change Request [REDACTED] to install the [REDACTED] [REDACTED] client upgrade on the [REDACTED] at [REDACTED]

Milestone 1-200 (Page 11)

Introduction (Page 11) shows the baseline change on May 30, 2017 for change request [REDACTED]. The [REDACTED] was upgraded to version [REDACTED].

The sections below shows the upgrade of the [REDACTED] to version [REDACTED] for the different devices types below except for the PCA-PIInterface devices.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Milestone 1-300 (Page 19)

The spreadsheet showing [REDACTED] mitigation plans [REDACTED] and [REDACTED] for the 2 [REDACTED] [REDACTED]e.

Milestone 1-400 (Page 20)

Change Request (31643) for the decommissioning of asse[REDACTED].

Milestone # 1 Completion verified.

Milestone 2: Service Management implementation.

Proposed Completion Date: July 28, 2017

Actual Completion Date: July 12, 2017

File 1, "RFC2017017777 Certification Package", Milestone 2 Submit. Evidentiary Document RFC2017017777 Milestone 2-100: Meeting with [REDACTED] Manager on July 12, 2017, to discuss [REDACTED] [REDACTED]. Meeting revealed that the new [REDACTED] [REDACTED] being considered did not include a triggering and escalation capability. The meeting also revealed that the search for a vendor providing [REDACTED] was being placed on hold.

Milestone 2-100 (Page 2)

Meeting notification on July 12, 2017 to discuss questions regarding change control... specifically what workflow capabilities exist that can act as triggers and escalations pertaining to NERC CIP time-based requirements.

Milestone # 2 Completion verified.

Milestone 3: Patch Deployment Verification checklist.

Proposed Completion Date: August 18, 2017

Actual Completion Date: August 17, 2017

File 1, “RFC2017017777 Certification Package”, Milestone 3 and 4 Submit. Evidentiary Document RFC2017017777 Milestones 3 and 4-100: [REDACTED] (SWI). Steps 1 through 4 of the SWI document the [REDACTED] for generating a patch deviation report from existing [REDACTED] baseline data (Milestone 4) and step 5 of the SWI documents how the results are collected in the [REDACTED] (Milestone 3).

[REDACTED] (Milestone 3) step 5 (Page 6)

This is the checklist for documentation of baseline changes, security controls testing and review. There is a tab for each asset type.

Milestone # 3 Completion verified.

Milestone 4: Scripting tool for [REDACTED] use.

Proposed Completion Date: September 29, 2017

Actual Completion Date: August 3, 2017

File 1, “RFC2017017777 Certification Package”, Milestone 3 and 4 Submit. Evidentiary Document RFC2017017777_Milestones 3 and 4-100: [REDACTED] (SWI). Steps 1 through 4 of the SWI document the scripting tool procedure for generating a patch deviation report from existing [REDACTED] baseline data (Milestone 4) and step 5 of the SWI documents how the results are collected in the [REDACTED] t (Milestone 3).

Scripting tool procedure (Milestone 4) steps 1 through 4 (Page 2)

Shows the first 4 steps of the [REDACTED] including the spreadsheet that is populated with the findings for each asset type in step 4.

Milestone # 4 Completion verified.

Milestone 5: [REDACTED]

Proposed Completion Date: December 7, 2017

Actual Completion Date: December 1, 2017

File 1, "RFC2017017777 Certification Package", Milestone 5 Submit. Evidentiary Document RFC2017017777 Milestone 5-100: The [REDACTED] [REDACTED] whitelist profiler capability is demonstrated in this document by defining a set of required/permited settings for a [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Milestone 5-100 (Page 2)

This shows for a [REDACTED] server how changes are reported on the unauthorized software report.

Milestone # 5 Completion verified.

The Mitigation Plan is hereby verified complete.



Date: [REDACTED]

Anthony Jablonski
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

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

Self Report

Entity Name: [REDACTED] ([REDACTED])

NERC ID: [REDACTED]

Standard: CIP-007-6

Requirement: CIP-007-6 R2.

Date Submitted: [REDACTED]

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED] [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: March 01, 2017 **Changed to April 28, 2017**

End/Expected End Date:

Reliability Functions: [REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]

Is Possible Violation still No
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Detailed Description:
Cause of Possible Violation:

In May 2017, while conducting a monthly [REDACTED]
[REDACTED] Quality Assessment (QA) review of [REDACTED] evidence for
March, it was discovered that several [REDACTED] ([REDACTED] group
patches successfully deployed to their Load Management System ([REDACTED] in the
test environment were not deployed in the production environment. Upon [REDACTED]
notification of this finding [REDACTED] filed a NERC Potential Violation Notification on
May 30, 2017 and conducted a detailed investigation which revealed the
following:

As per current patch management process [REDACTED] patch evaluations are
conducted on the 1st work day of a calendar month and deployed or mitigation
plans are created/updated within 35 days of the evaluation. [REDACTED] [REDACTED] has a
patch source of [REDACTED] who distribute software updates as a package on
the second Tuesday of every month, referred to in this report as "Patch
Tuesday". The initial [REDACTED] patch evaluation of [REDACTED] "February Patch
Tuesday" package was conducted and approved for deployment to the [REDACTED] in
March.

Shortly after the [REDACTED] patch evaluation, [REDACTED] unexpectedly announced that
the "February Patch Tuesday" package was incomplete, withdrew the package
and on March 14, 2017 re-released a corrected package as their "March Patch
Tuesday" package, thereby changing their normal package release cadence.

Self Report

Due to this change in patching cadence, [REDACTED] decided to use the "March Patch Tuesday" package for their March evaluation and March deployment to the [REDACTED]. The "March Patch Tuesday" package was deployed to the [REDACTED] in the test environment later in the month than usual, but without any issues.

March patches were then applied in the production environment, however they were applied using the originally approved "February Patch Tuesday" package, the end result being that [REDACTED] applied more current patches to the [REDACTED] in the test environment than in the production environment. March patches were not applied within the required 35 calendar days of evaluation resulting in possible non-compliance (PNC) with CIP-007 R2. P2.3.

Prior to the discovery of this delta in patch packages, the [REDACTED] was removed as a NERC CIP BES Cyber Asset (BCA) and disconnected from all networks in late May 2017. It was originally assumed to be a NERC CIP asset based on its function and location in the [REDACTED] [REDACTED] however, upon evaluation, it did not meet the load-shed criteria for NERC CIP standards and was consequently decommissioned from the NERC CIP Asset List.

Extent of Condition. During the investigation, [REDACTED] discovered that several assets were not running the latest version of [REDACTED] client software ([REDACTED] used to provide remote management services required for server and workstation maintenance). The missing assets were added to the automated [REDACTED] tool which updated the assets to the current version of [REDACTED] on May 07, 2017.

Root Cause of Possible Non-Compliance:

On June 08, 2017 an [REDACTED] [REDACTED] was conducted to establish the PNC timeline. A follow-up [REDACTED] was conducted on June 14, 2017 to obtain additional information, develop a problem description and determine the root cause(s). The problem was identified as applicable patches not being applied within 35 days of the completed patch evaluation resulting in PNC with CIP-007-6 R2. P2.3. The cause for the PNC was determined to be two patch groups being maintained in the patch evaluation and deployment process; one for use in the test environment and one for use in the production environment. The change in [REDACTED] package release cadence - a first time occurrence for [REDACTED] - compressed the patch evaluation and deployment process and created two patch groups that were out of sequence. These factors led to a breakdown in the patch evaluation and deployment process handoff and subsequent deployment of two different packages.

The Extent of Condition Root Cause was determined to be a manual process was being used for updating [REDACTED] using a static list of assets. The static list of assets was determined to be incomplete. The [REDACTED] group has since integrated all the windows assets into the automated patch management tool which will eliminate errors experienced using the manual process.

How was the violation discovered?

During an [REDACTED] [REDACTED] QA review of the March [REDACTED] provided evidence conducted on May 4, 2017 it was discovered that patches deployed in the test environment were different from the patches deployed in production.

Timeline:

03/01/2017: [REDACTED] group completes security patch evaluation and prepares approved patch groups for test and production environments.
03/01/2017 to 03/13/2017: [REDACTED] unexpectedly announces the "February Patch Tuesday" package is incomplete and withdraws the package.
03/14/2017: [REDACTED] re-issues "February Patch Tuesday" package as their "March Patch Tuesday" package.
03/23/2017: [REDACTED] decides to use the "March Patch Tuesday" package for their March evaluation and March deployment to [REDACTED] assets in the test environment.
03/31/2017: [REDACTED] applies March patches in the production environment using the originally approved "February Patch Tuesday" package.

Self Report

05/04/2017: [REDACTED] QA review of March [REDACTED] provided evidence reveals patches deployed in the test environment are different from the patches deployed in production. [REDACTED] notifies the [REDACTED] group who initiate an investigation.

05/07/2017: During extent of condition investigation, [REDACTED] discovers 6 servers and 6 work stations were not running the latest version of [REDACTED] client software ([REDACTED]). The missing assets were added to the automated patch management tool and updated to the current version of [REDACTED].

05/30/2017: [REDACTED] initiates a NERC Potential Violation Notification of its investigation and findings.

05/31/2017: [REDACTED] assets decommissioned from NERC CIP Asset List for unrelated reasons and disconnected from all networks.

06/08/2017: [REDACTED] conducted to establish the PNC timeline.

06/14/2017: [REDACTED] conducted to obtain additional information, develop a problem description and determine the root cause(s).

Mitigating Activities:

Description of Mitigating Activities:
Activities and Preventative Measure: As stated in the detailed description, prior to the discovery of this delta in patch packages, the [REDACTED] was removed as a NERC CIP BES Cyber Asset (BCA) and disconnected from all networks in mid-May 2017. The affected assets with outdated versions of [REDACTED] were updated to the current version on May 07, 2017.

Preventive Measures:

The handoff between patch evaluation and patch deployment will utilize the same patch set to eliminate patch set version control issues.

The [REDACTED] group has integrated all applicable Cyber Assets that are updateable and for which a patching source exists into the automated patch management tool which will eliminate errors experienced using previous manual processes.

[REDACTED] has also implemented an automated baseline comparison script used immediately following patch deployments to generate a deviation report for all third party software on all assets. The deviation report will be used as a preventive review control to validate all patching was successfully completed as intended within the 35-day requirement.

Date Mitigating Activities May 31, 2017
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 considered to be high. [REDACTED] has a documented process for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches within 65 calendar days of the evaluation completion.

The actual impact to the BPS is low. The [REDACTED] was originally assumed to be a NERC CIP asset based on its function and location in the [REDACTED] however, upon evaluation, did not meet the load-shed criteria for NERC CIP standards and was consequently decommissioned from the NERC CIP Asset List on May 31, 2017. The [REDACTED] group corrected the incomplete list of assets being scanned by [REDACTED] patch management tool used to identify missing and outdated software and manually updated the [REDACTED] client software on the affected assets on May 07, 2017.

Self Report

Risk Assessment of Impact to BPS: The risk of Impact to the BPS has been identified as low. The [REDACTED] client software provide remote management services required for server and workstation maintenance. Access to these services are restricted to system admins and intended users.

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
RFC2017017839	CIP-007-6 R2.	

Mitigation Plan Submitted On: [REDACTED]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: July 06, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [REDACTED] On:

Mitigation Plan Completion Verified by RF On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

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

- (1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
 - (2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
 - (3) The cause of the Alleged or Confirmed Violation(s).
 - (4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
 - (5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
 - (6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
 - (7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
 - (8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
 - (9) Any other information deemed necessary or appropriate.
 - (10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
 - (11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.
- The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.
 - This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.
 - If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.
 - Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.
 - Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.
 - The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [REDACTED]

NERC Compliance Registry ID: [REDACTED]

Address: [REDACTED]

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

Name: [REDACTED]

Title: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Violation(s)

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

Violation ID	Date of Violation	Requirement
Requirement Description		
RFC2017017839	03/01/2017	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:

Brief Description: (What happened?)

In May 2017, while conducting a monthly review of evidence for March, it was discovered that several group patches successfully deployed to their Load Management System in the test environment were not deployed in the production environment. Upon notification of this finding filed a NERC Potential Violation Notification on May 30, 2017, and conducted a detailed investigation which revealed the following:

As per current patch management process patch evaluations are conducted on the 1st work day of a calendar month and deployed or mitigation plans are created/updated within 35 days of the evaluation. has a patch source of who distribute software updates as a package on the second Tuesday of every month, referred to in this report as "Patch Tuesday". The initial patch evaluation of "February Patch Tuesday" package was conducted and approved for deployment to the in March.

Shortly after the patch evaluation, unexpectedly announced that the "February Patch Tuesday" package was incomplete, withdrew the package and on March 14, 2017, re-released a corrected package as their "March Patch Tuesday" package, thereby changing their normal package release cadence.

Due to this change in patching cadence, decided to use the "March Patch Tuesday" package for their March evaluation and March deployment to the. The "March Patch Tuesday" package was deployed to the in the test environment later in the month than usual, but without any issues.

March patches were then applied in the production environment. However, the patches were applied using the originally approved "February Patch Tuesday" package, with the end result being that applied more current patches to the in the test environment than in the production environment.

Prior to the discovery of this delta in patch packages, the was removed as a NERC CIP BES Cyber Asset (BCA) and disconnected from all networks in late May 2017. It was originally assumed to be a NERC CIP asset based on its function and location in the. However, upon evaluation, it did not meet the load-shed criteria for NERC CIP standards and was consequently decommissioned from the NERC CIP Asset List.

Extent of Condition. During the investigation, discovered that several assets were not running the latest version of client software used to provide remote management services required for server and workstation maintenance. The missing assets were added to the automated patch management tool which updated the assets to the current version of on May 07, 2017.

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

On June 08, 2017, an was conducted to establish the PNC timeline. A follow-up was conducted on June 14, 2017 to obtain additional information, develop a problem description and determine the root cause(s). The problem was identified as applicable patches not being applied within 35 days of the completed patch evaluation resulting in PNC with CIP-007-6 R2 P2.3. The cause for the PNC was determined to be two patch groups being maintained in the patch evaluation and deployment process; one for use in the test environment and one for use in the production environment. The change

in [REDACTED] package release cadence - a first time occurrence for [REDACTED] - compressed the patch evaluation and deployment process and created two patch groups that were out of sequence. These factors led to a breakdown in the patch evaluation and deployment process handoff and subsequent deployment of two different packages.

The Extent of Condition Root Cause was determined to be a manual process was being used for updating [REDACTED] using a static list of assets. The static list of assets was determined to be incomplete. The [REDACTED] group has since integrated all the [REDACTED] assets into the automated patch management tool [REDACTED]. Tool usage will eliminate errors experienced using the manual process.

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

How was the violation discovered?

During an [REDACTED] [REDACTED] QA review of the March [REDACTED] provided evidence conducted on May 4, 2017 it was discovered that patches deployed in the test environment were different from the patches deployed in production.

The handoff between patch evaluation and patch deployment will utilize the same patch set to eliminate patch set version control issues.

The [REDACTED] group has integrated all applicable Cyber Assets that are updateable and for which a patching source exists into the automated patch management tool which will eliminate errors experienced using previous manual processes.

[REDACTED] has also implemented an automated baseline comparison script used immediately following patch deployments to generate a deviation report for all third-party software on all assets. The deviation report will be used as a preventive review control to validate all patching is successfully completed as intended within the 35-day requirement

Plan Details

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

Milestone 1- The handoff between patch evaluation and patch deployment will utilize the same patch set to eliminate patch set version control issues. The use of the same patch set was implemented on May 31, 2017. By using the same patch set, further clarity is introduced in the patching process and the avoidance of confusion enhances communication and reduces ambiguity.

Milestone 2- The [REDACTED] group has integrated all applicable Cyber Assets that are updateable and for which a patching source exists into the automated patch management tool which will eliminate errors experienced using previous manual processes. This integration happened on May 31, 2017. A report showing all integrated applicable Cyber Assets that are updateable and for which a patching source exists in the automated patch management tool will be provided as evidence.

Milestone 3- The [REDACTED] group has also implemented an automated baseline comparison script used immediately following patch deployments to generate a deviation report for all third-party software on all assets. The deviation report will be used as a preventive review control to validate all patching was successfully completed as intended within the 35-day requirement. A [REDACTED] catcher file is generated when the [REDACTED] and third-party software assessment has been completed. For each evaluated patch source, an entry is created in the [REDACTED] catcher file which specifies the name of the patch and the Patch version number. [REDACTED] baseline data is prepared and the CIP-010 data is processed using the [REDACTED] catcher file. The [REDACTED] script which is used to generate the Patch Deviation Report and applies a filter to the CIP-010 data to determine if the software on each asset is at the correct version, and which software has yet to be patched. The final evidence of compliance is not generated until all required patches have been applied and the Patch Deviation Report shows the expected output. The implementation of the automated baseline comparison script has been implemented as of June 23, 2017 into the patch management process. A deviation report for all third-party software assets will be provided as evidence. This deviation report is used to verify that all patches have been applied, and if there is a deviation, further investigation is initiated, and corrective action taken in a timely manner.

Milestone 4- The improved embedded control deviation report was incorporated by the [REDACTED] group into the process documentation as of June 23, 2017. Evidence of milestone completion is the revised and issued process document.

Milestone 5- A reconciliation to confirm the inclusion of all [REDACTED] [REDACTED] assets from CIP002 asset list exist in the [REDACTED] patch management database as of July 6, 2017. The evidence is an excel spreadsheet which compares the [REDACTED] database files and [REDACTED] Assets by Patch group is the evidence of milestone completion.

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 06, 2017

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

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
--------------------	-------------	---	------------------------	--	---------------------------

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: Use of same patch set	The handoff between patch evaluation and patch deployment will utilize the same patch set to eliminate patch set version control issues.	05/31/2017	05/31/2017		No
Milestone 2: All Cyber Assets added to the automated patch management tool	Integrate all applicable Cyber Assets that are updateable and for which a patching source exists into the automated patch management tool.	05/31/2017	05/31/2017		No
Milestone 3: Implementation of an automated baseline comparison script	Generates a deviation report for all third-party software on all assets.	06/23/2017	06/23/2017		No
Milestone 4: Update patching process	Update the patching process to include embedded control deviation report	06/23/2017	06/23/2017		No
Milestone 5: Patch management tool reconciliation	Reconcile CIP002 list to ensure that windows assets are in	07/06/2017	07/06/2017		No

Additional Relevant Information

Reliability Risk

Reliability Risk

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

The potential impact to the BES is considered to be high. [REDACTED] has a documented process for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches within 35 calendar days of the evaluation completion.

The actual impact to the BES is low. The [REDACTED] was originally assumed to be a NERC CIP asset based on its function and location in the [REDACTED] ([REDACTED]). However, upon evaluation, did not meet the load-shed criteria for NERC CIP standards and was consequently decommissioned from the NERC CIP Asset List on May 31, 2017. The [REDACTED] group corrected the incomplete list of assets being scanned by their patch management tool used to identify missing and outdated software and manually updated the [REDACTED] client software on the affected assets on May 07, 2017.

Prevention

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

The improvements we have already outlined and implemented in our process will help to strengthen our patch management process. By taking a proactive approach to try and find issues early in the patching process and being able to react to them in a timely manner will strengthen the patching process. This will help to ensure that all our patches are applied in a timely manner and all relevant patches are applied to both the [REDACTED] environments. This will further ensure and maintain [REDACTED] compliance with CIP-007-6 R2 P2.3.

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

ReliabilityFirst

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] [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): RFC2017017839

Mitigated Standard Requirement(s): CIP-007-6 R2.

Scheduled Completion as per Accepted Mitigation Plan: July 06, 2017

Date Mitigation Plan completed: July 06, 2017

RF Notified of Completion on Date: [REDACTED]

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017839 Certification Package.zip	A zip file "RFC2017017839 Certification Package.zip" contains the following: Cover sheet for the whole package supporting evidence for each milestone.	1,165,932

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 RFC2017017839

██████████ (██████████)

Standard/Requirement: CIP-007-6 R2

NERC Mitigation Plan ID: RFCMIT013016

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	Mitigation Plan Submittal	RF Acceptance	NERC Approval	Certification Submittal	Date of Completion
██████████ ██████████	██████████	██████████		██████████	07/06/17

Description of Issue

In May 2017, while conducting a monthly ██████████ (██████████) ██████████ of ██████████ evidence for March, it was discovered that several ██████████ (██████████) group patches successfully deployed to their Load Management System (██████████) in the test environment were not deployed in the production environment. Upon ██████████ notification of this finding ██████████ filed a NERC Potential Violation Notification on May 30, 2017, and conducted a detailed investigation which revealed the following:

As per current patch management process ██████████ patch evaluations are conducted on the 1st work day of a calendar month and deployed or mitigation plans are created/updated within 35 days of the evaluation. ██████████ ██████████ has a patch source of ██████████ who distribute software updates as a package on the second Tuesday of every month, referred to in this report as "Patch Tuesday". The initial ██████████ patch evaluation of ██████████ "February Patch Tuesday" package was conducted and approved for deployment to the ██████████ in March.

Shortly after the ██████████ patch evaluation, ██████████ unexpectedly announced that the "February Patch Tuesday" package was incomplete, withdrew the package and on March 14, 2017, re-released a corrected package as their "March Patch Tuesday" package, thereby changing their normal package release cadence.

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

Due to this change in patching cadence, [REDACTED] decided to use the "March Patch Tuesday" package for their March evaluation and March deployment to the [REDACTED]. The "March Patch Tuesday" package was deployed to the [REDACTED] in the test environment later in the month than usual, but without any issues.

March patches were then applied in the production environment. However, the patches were applied using the originally approved "February Patch Tuesday" package, with the end result being that [REDACTED] applied more current patches to the [REDACTED] in the test environment than in the production environment.

Prior to the discovery of this delta in patch packages, the [REDACTED] was removed as a NERC CIP BES Cyber Asset ([REDACTED]) and disconnected from all networks in late May 2017. It was originally assumed to be a NERC CIP asset based on its function and location in the [REDACTED] ([REDACTED]). However, upon evaluation, it did not meet the load-shed criteria for NERC CIP standards and was consequently decommissioned from the NERC CIP Asset List.

Extent of Condition. During the investigation, [REDACTED] discovered that several assets were not running the latest version of [REDACTED] client software ([REDACTED]) used to provide remote management services required for server and workstation maintenance. The missing assets were added to the automated patch management tool which updated the assets to the current version of [REDACTED] on May 07, 2017.

The cause for the PNC was determined to be two patch groups being maintained in the patch evaluation and deployment process; one for use in the test environment and one for use in the production environment. The change in [REDACTED] package release cadence - a first time occurrence for [REDACTED] - compressed the patch evaluation and deployment process and created two patch groups that were out of sequence. These factors led to a breakdown in the patch evaluation and deployment process handoff and subsequent deployment of two different packages.

The Extent of Condition Root Cause was determined to be a manual process was being used for updating [REDACTED] using a static list of assets. The static list of assets was determined to be incomplete. The [REDACTED] group has since integrated all the [REDACTED] assets into the automated patch management tool [REDACTED]. Tool usage will eliminate errors experienced using the manual process.

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	RFC2017017839 Certification Package	CIP-007-6 R2

Verification of Mitigation Plan Completion

Milestone 1: Use of same patch set.

File 1, “*RFC2017017839 Certification Package*”, Milestone 1-Submit, Pages 1 and 2, show and describe how the entity will utilize the same patches among their [REDACTED] testing system as well as their production environment.

Milestone # 1 Completion verified.

Milestone 2: All Cyber Assets added to the automated patch management tool.

File 1, “*RFC2017017839 Certification Package*”, Milestone 2- Submit, Pages 2 through 10, illustrate that updateable applications that have patch sources were integrated into the entity automated patch management tool and also shows that [REDACTED] assets are in sync with the [REDACTED] database.

Milestone # 2 Completion verified.

Milestone 3: Implementation of an automated baseline comparison script.

File 1, “*RFC2017017839 Certification Package*”, Milestone 3- submit, Page 2, shows that all applications/ systems required to be patched have been patched via their log catcher system.

Milestone # 3 Completion verified.

Milestone 4: Update patching process.

File 1, “*RFC2017017839 Certification Package*”, Milestone 4-submit, Page 2, shows that the entity has added 2 additional controls to their patching process in order check for deviations.

Milestone # 4 Completion verified.

Milestone 5: Patch management tool ([REDACTED]) reconciliation.

File 1, “RFC2017017839 Certification Package”, Milestone 5-Submit, Pages 2 through 5, show that [REDACTED] devices have been validated to be contained within the [REDACTED] [REDACTED] [REDACTED] as determined by the entity.

Milestone # 5 Completion verified.

The Mitigation Plan is hereby verified complete.

A handwritten signature in black ink, appearing to read "Tony Purgar". The signature is fluid and cursive, with the first name "Tony" and last name "Purgar" clearly distinguishable.

Date: [REDACTED]

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [REDACTED] ([REDACTED])

NERC ID: [REDACTED]

Standard: CIP-007-6

Requirement: CIP-007-6 R2.

Date Submitted: August 29, 2018

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED] [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: June 21, 2018

Changed to June 22, 2018

End/Expected End Date: July 20, 2018

Reliability Functions: [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Is Possible Violation still No
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and *Date violation was contained:
Cause of Possible Violation: The patch evaluation, CIP-007 R2.2, for the June Patch Cycle was completed on June 22, 2018. The task was due on June 21.

The application of patches, CIP-007 R2.3, for the May Patch Cycle of the [REDACTED] Physical Access Control System (PACS), was completed on July 20, 2018. The task was due on June 21.

*Detailed Description:
Current Practice: [REDACTED] maintains a NERC asset patching program following a monthly cadence. The processes initiates with a monthly review of patch sources and an evaluation of security relevant and applicable patches, updates, firmware. The results of the evaluation are documented and include, for each potential installation, four possible outcomes:

Install applicable patches within 35 calendar days (Deploy) - If, through evaluation, patches are determined to be applicable, SMEs choose Deploy in the assessment (evaluation) template and they install those patches within 35 calendar days of the evaluation.

Create or revise a dated mitigation plan when the applicable patches cannot be installed within 35 calendar days (Mitigate) - If, through evaluation, patches are determined to be applicable but cannot be installed within 35 calendar

Self Report

days, SMEs choose Mitigate in the [REDACTED] and create a new mitigation plan or update an existing mitigation plan. The plan must be created or updated within 35 days of the evaluation.

Patches are not to be deployed (Do Not Deploy) - If, through evaluation, patches are determined to be applicable but cannot be deployed because, for example, a vendor reports that the patch is not compatible with a critical application, SMEs choose Do Not Deploy in the [REDACTED]. Note that this option also includes the creation of a dated mitigation plan.

Install some applicable patches and open/revise a mitigation plan(s) for others (Combination) - If, through evaluation, patches are determined to be applicable but only some of them can be applied within 35 days, SMEs choose Combination: Deploy and Mitigate in the [REDACTED] and, within 35 days of the evaluation, install patches that can be installed and create a new mitigation plan or update an existing mitigation plan.

Incident Description: The [REDACTED] Physical Access Control System (PACS) BCS has never had violation for CIP007 R2 in the past. A new SME (SME) started with [REDACTED] on April 21st and was assigned to CIP compliance activities for PACS. The former SME had an informal handoff to the SME, with training including allowing the SME to shadow her during patch installations and related tasks, all performed May. The former SME also introduced the SME to the monthly [REDACTED] workbook and related templates.

All PACS patches evaluated in May were recorded as "Deploy," meaning they were all to be installed in June (within 35 days of the evaluation). The SME began the installations on June 11, 2018. The target installation due date, as per [REDACTED] practice, was five days before the compliance requirement. The compliance due date was June 21, 2018. The SME utilized a standard patching application, [REDACTED] Patch for [REDACTED] (formerly [REDACTED]) to perform the patch installations. The SME followed the [REDACTED] Job Aid and instructed [REDACTED] Patch to apply multiple security patches to all PACS systems concurrently. This action resulted in [REDACTED] Patch "hanging", multiple patches failing, and some system instability. The SME contacted the former SME for support. The two cleared the [REDACTED] Patch errors and attempted to resume the patching process. At 6:00pm, the scheduled change window closed and all patching activities ceased, with the server patches having not been applied.

Reminders of the PACS task due dates were announced in the June 14, 2018 [REDACTED]; however, the SME was not present. The SME was then notified on both June 20 and June 21, via email, that compliance tasks were coming due. The SME responded, on June 21, that she would publish evidence later that day for some of the tasks.

On June 21, a weekly [REDACTED] was held. The PACS SME was informed that a CIP-010 2.1 requirement was due on June 22. The SME stated that she had not yet completed the requirement as she had technical problems related to her electronic access and she was unable to run the required scripts. She then mentioned that she had been advised that she needed to complete a mitigation plan because her patching was not fully successful. A [REDACTED] representative notified the SME that a mitigation plan was not applicable to the situation and her patches and other tasks must be completed.

On June 22, representatives of [REDACTED] as well as several SMEs from technical areas, assisted the SME to continue patching and correct permission errors. Corrections to permissions were only partially successful, however the former PACS SME completed the baseline-related tasks on her own workstation, with her credentials. The PACS system was successfully stabilized and a change order was opened to complete any remaining patches. Those patches were completed on June 20, 2018.

On June 22, the SME also completed her patch evaluation for the next patch cycle.

Self Report

***What is the problem?**

PACS systems were not patched within the required 35 days of the patch evaluation, with 149 patches installed on the 36th day and 24 patches installed on the 63rd day. Similarly, the patch evaluation for the June patch cycle was not completed within 35 days of the previous patch evaluation, completed instead on the 36th day.

***Root Cause of Possible Violation:**

The root cause of the problem was found to be an ad hoc and unsuccessful knowledge transfer to the new/current PACS SME, combined with insufficient documentation.

***How was the violation discovered?**

The activities surrounding the violations were known to the SME, however the violations themselves were discovered within the monitoring and review portions of the [REDACTED] [REDACTED]

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

This noncompliance is related to both documentation and performance.

The [REDACTED] Job Aid was found to not specify how many systems to deploy to at one time. However, the screenshot instruction is configured to deploy patches to six systems concurrently. The six systems displayed include all four PACS test servers and two test workstations, including what, in Production, would be both primary and failover machines. A separate document, [REDACTED] Server Patching, reads to install patches to one server at a time, but gives no guidance regarding the use of the patching tool. Neither document specifically references the other.

It was determined that the PACS SME did not have sufficient training and guidance to successfully complete the required tasks on her own, without a reliance on documentation or the former PACS SME.

***Timeline:**

April 21, 2018 - A former [REDACTED] contractor ([REDACTED] role) was hired as a [REDACTED] contractor and planned PACS SME.

May, 2018 through early June, 2018 - PACS training and transitioning took place, with the SME role transitioning from the former SME to the current SME (SME).

June 11, 2018 - Patch installation for the May patch cycle, those patches evaluated in May, was attempted by the SME. Multiple patches failed and the patch installation tool "hung."

June 14, 2018 - At the weekly [REDACTED] Meeting, it was announced that PACS had multiple [REDACTED] tasks due on June 16 and 17. No representatives of PACS were present. An [REDACTED] task was made to contact the former PACS SME, as [REDACTED] documents still listed her as the SME.

June 20, 2018 - SME and backup SME, also new, were notified by [REDACTED] via email, that three tasks were overdue. The tasks were CIP-007 R2.1, CIP-007 R2.2, and CIP-010 2.1, due on June 16, June 16, and June 17 respectively. The SME responded to the email and stated that she would upload the evidence package today (June 20).

June 21, 2018 - At the weekly [REDACTED] (2:00pm), SME was questioned regarding the status of the PACS baseline.

June 22, 2018 - [REDACTED] representatives worked with the SME to continue the patching cycle and baseline creation.

June 22, 2018 - PACS was stabilized.

June 22, 2018 - [REDACTED] confirmed the patch installation and patch evaluation PNCs.

June 22, 2018 - SME and former SME, together, completed the baseline.

July 11, 2018 - SME opened a [REDACTED] emergency change order to complete the final patch installations, three patches for each of the PACS servers.

July 16, 2018 - The emergency change order received its final approval.

July 20, 2018 - The final patch installations were completed.

Self Report

August 13, 2018 - SME NERC Onboarding completed.
August 24, 2018- Updated PACS documentation completed, approved, and communicated.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Immediate Correcting Activities:
All systems were patched to the highest level possible and stabilized. The remaining patches were installed following confirmation of a stable environment. COMPLETED
Included as Milestone 1- Submit.

Mitigating Activities:
Verify completion of the May, 2018 PACS Patch Cycle.
--- The May Patch Evaluation and associated [REDACTED] baseline and deviation reports were reviewed.
--- Included as Milestone 1- Submit.
Correct the Job Aid, combining documentation and/or clarifying the instructions - Completed.
--- Three documents, two SWIs and one job aid, were combined and corrected to create the [REDACTED] SWI Workstation and Server Patching.
--- Included as Milestone 2 - Submit.
Allow the PACS SME to participate in the NERC Onboarding Process - Completed.
--- The NERC Onboarding Process was utilized and followed for the current PACS SME. The Process was completed on August 13, 2018.
--- Included as Milestone 3 - Submit.

Preventative Measures:
Published the formal NERC CIP SME Onboarding Process - Completed.
--- Developed and submitted for RFC2018019428.
--- Included as Milestone 4 - Submit.
The NERC Onboarding Process will be utilized for all incoming NERC SMEs - Implemented.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Moderate
Actual Impact to BPS: Minimal

Description of Potential and Actual Impact:
Actual Impact to BPS: The PACS experienced some instability, however no failures of physical access controls are known to exist as related to the identified activities.

Potential Impact:
Failure to apply all applicable security patches to the [REDACTED] PACS in a timely manner and/or failure to follow safe and approved installation procedures increases the risks of physical security compromise, failure to detect unauthorized entry or exit, and inadequate investigation of security incidents.

Risk Assessment of Impact to BPS: The potential impact to the PACS was high as the System did experience some instability. The application of layered security, including guards, mechanical locks, cameras, and alarms served to mitigate the risk to BES assets.

Self Report

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Milestone 1 - Submit.pdf		197,281
Entity	Milestone 1 - Baseline.pdf		482,999
Entity	Milestone 1 - Evaluation.xlsx		52,293
Entity	Milestone 2 - Submit.pdf		961,538
Entity	Milestone 3 - Submit.pdf		1,240,814
Entity	Milestone 4 - Submit.pdf		2,515,963

Mitigating Activities Verification for RFC2018020386

Standard/Requirement: CIP-007-6 R2

NERC Registry ID: [REDACTED]

Method of Disposition: Not yet determined

Relevant Dates			
Initiating Document	Submittal of Activities	RF Acceptance	Date of Completion
Self-Report 08/29/18	08/29/18	02/25/19	08/24/18

Description of Issue

[Mitigating Activity Task RFC2018020386](#)

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	Milestone 1 Baseline	CIP-007-6 R2
File 2	Milestone 1 Evaluation	CIP-007-6 R2
File 3	Milestone 1 Submit	CIP-007-6 R2
File 4	Milestone 2 Submit	CIP-007-6 R2
File 5	Milestone 3 Submit	CIP-007-6 R2
File 6	Milestone 4 Submit	CIP-007-6 R2
File 7	RFC2018020386 July violation	CIP-007-6 R2
File 8	RFC2018020386 RFI Response	CIP-007-6 R2

Verification of Mitigating Activity Completion

Mitigating Activity 1: Verify the Completion of the May, 2018 Patch Cycle, PACS Patch Cycle

File 1, “*Milestone 1 - Baseline,*” Pages 1 through 224, shows a list of patches applied. The file can be searched for patch numbers from the evaluation. File 2, “*Milestone 1 – Evaluation,*” provides evidence into patching source and patch evaluation.

Mitigating Activity # 1 Completion verified.

Mitigating Activity 2: Correct the Job-Aid associated with Mitigating Activity 1

File 4, “*Milestone 2- Submit,*” Pages 2 through 13, show the correction to the [REDACTED] Server OS Patching job aid and communication of changes to effected personnel via email.

Mitigating Activity # 2 Completion verified.

Mitigating Activity 3: Allow PACS SME to participate in the NERC Onboarding Process

File 5, “*Milestone 3- Submit,*” Pages 2 through 4, show the formal signed/ approved onboarding of an entity “PACS SME” as per their internal training and knowledge transfer.

Mitigating Activity # 3 Completion verified.

Mitigating Activity 4: Publish Formal NERC Onboarding Process

File 6, “*Milestone 4-Submit,*” Pages 5 through 35, show the formalized onboarding process of entity CIP SMEs in order to provide them the fundamental skills for operating within the CIP space.

Mitigating Activity # 4 Completion verified.

The Mitigating Activities is hereby verified complete.



Date: 4/2/19

Tom Scanlon
Counsel
ReliabilityFirst Corporation

Attachment 10

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

- 10.a The Entity's Self-Report (RFC2017017548);
- 10.b The Entity's Mitigation Plan designated as RFCMIT012983 submitted [REDACTED];
- 10.c The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
- 10.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
- 10.e The Entity's Self-Report (RFC2018019469);
- 10.f The Entity's Mitigation Plan designated as RFCMIT013708 submitted [REDACTED];
- 10.g The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
- 10.h ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
- 10.i The Entity's Self-Report (RFC2018020086);
- 10.j The Entity's Mitigation Plan designated as RFCMIT014196 submitted [REDACTED]
[REDACTED];
- 10.k The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
- 10.l ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED];
- 10.m The Entity's Self-Report (RFC2019021564);
- 10.n The Entity's Mitigation Plan designated as RFCMIT014560 submitted [REDACTED];
- 10.o The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
- 10.p ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED]

Self Report

Entity Name: [REDACTED] ([REDACTED])

NERC ID: [REDACTED]

Standard: CIP-007-6

Requirement: CIP-007-6 R4.

Date Submitted: [REDACTED]

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED] [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: May 03, 2017 **Changed to July 1, 2016**

End/Expected End Date:

Reliability Functions: [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Is Possible Violation still No
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: Following a scheduled QA assessment, performed by [REDACTED] early March 2017, it was noted that cyber assets belonging to 3 [REDACTED] Business Units: [REDACTED] [REDACTED] [REDACTED] and [REDACTED] were not monitored for security incidents, logged (centrally, using [REDACTED] or locally), and sending out alerts to appropriate individuals when necessary. As a result, logs were not kept for 90 days as required in CIP007-6 R4.3 Also, the affected business units did not receive alerts from the [REDACTED] ([REDACTED]) team responsible for configuring and monitoring the affected assets.

Instance one: At the [REDACTED] it was discovered that 12 [REDACTED] Servers, categorized as BCAs, managing the VM environment, were configured to capture security logs as per R4.1. Yet, the assets were not appropriately configured to send alerts to correct units and personnel. This therefore, constitutes a violation of CIP007-6 R4.2. In addition, logs were not kept for 90 days as required in CIP007-6 R4.3. [REDACTED] were decommissioned on 3/17/17 using Change Order [REDACTED] and were removed from CIP002 list on 3/27/2017. Alerts were not sent because incorrect protocols were used during configuration and the firewalls were misconfigured. As a result, security alerts generated from these assets were routed to the wrong recipients and storage. Another reason attributed to this violation is that [REDACTED] (Legacy) server and [REDACTED] (New) were both used in parallel, with different asset naming conventions. This situation led to a mismatch of asset IDs during configuration that further compounded the problem.

Self Report

As of March 13, 2017, all the configuration and protocol errors are correct and the assets are configured to send alerts to the appropriate units and recipients. A trial alert was successfully generated on March 15 for a failed login attempt. The trial confirms that the mitigation effort is effective.

Instance two: [REDACTED] identified [REDACTED] [REDACTED] servers capable of local logging only, were not manually reviewed every 15 calendar days as required. This situation is a violation of CIP-007 R4.4. These assets are now decommissioned and require no further corrective action.

Instance three: In July 2016, a senior engineer with the [REDACTED] [REDACTED] unit sent [REDACTED] of assets that needed to be monitored for security incidents to the [REDACTED] team. It was discovered that while other assets are logged, no log existed for [REDACTED] assets at [REDACTED]. Upon further investigation conducted by the senior network engineer, it was noted that the vendor [REDACTED] left a command on the devices since their inception, that turned logging off. The logging function was never turned back on; as a result, logs were not being generated from July 1st 2017 when the facility came into compliance till the discovery was made and fixed on January 12, 2017. Upon this discovery, the senior engineer notified [REDACTED] on January 25, 2017 of the failure. As a result, the assets were not monitored, nor were alerts generated for security events as required in CIP007-6 R4.2. This command was corrected to initiate logging.

Root Cause of Possible Violation:

Instance 1: The root cause of this violation at the [REDACTED] is as a result of firewall misconfiguration due to the use of a wrong protocol, which led to logs being routed to the wrong locations;

Instance 2: The root cause of this violation at the [REDACTED] unit is attributed to a gap in the [REDACTED] monitoring process that did not provide business units with adequate insight into monitoring activities performed.

Instance 3: The vendor [REDACTED] disabled the logging in order to execute the troubleshooting however after the task was completed the vendor did not switch on the logging back to its original configuration.

How was the violation discovered?

Instance One and Two: This possible violation was discovered during a routine QA assessment performed by [REDACTED] that began in January 2017.

Instance Three: This possible violation was discovered when the [REDACTED] team made an ad hoc confirmation inquiry to a [REDACTED] Analyst in December 2016, regarding the status of their assets being logged and monitored by the [REDACTED] group. He was told that no log was available for the [REDACTED] BCA assets involved in question.

Timeline:

July 2016 [REDACTED] provided list of [REDACTED] of assets that needed to be logged and monitored, to the [REDACTED] team in a bid to enhance the security of the devices

12/22/2016 During Phase 2 of Network engineering equipment upgrade, senior network engineer inquired to know if logging is still enabled. He found out that it wasn't.

January 2017 [REDACTED] began scheduled QA assessment of [REDACTED] BCS and facilities

January 12, 2017 [REDACTED] Senior engineer created a Change Order to remove vendor command that prevented [REDACTED] from being sent out.

January 12, 2017 Change Order to remove vendor command that prevented [REDACTED] from being sent out was closed after the command was successfully removed.

January 25, 2017 [REDACTED] notified [REDACTED] of PV that logging is not configured.

January 25, 2017 Assets noted in Instance three started logging successfully to [REDACTED]

February 15, 2017 Foss Gen noted that alerts are not being received, PV

Self Report

notification sent to [REDACTED]
 February 24, 2017 [REDACTED] filed a PV notification upon discovering that logging is not configured as expected.
 March 13, 2017 [REDACTED] [REDACTED] corrected all firewall and routing misconfigurations regarding predefined systems and security incident logs that may impact proper routing of alerts.
 March 13, 2017 [REDACTED] [REDACTED] established a defined location for storing collected logs ([REDACTED])
 March 17, 2017 Assets noted in Instance two, [REDACTED] were decommissioned on 3/17/17 using Change Order [REDACTED]
 March 15, 2017 [REDACTED] [REDACTED] team generated test failed login attempts to confirm that relevant logs and alerts are indeed generated and sent to the appropriate contacts.
 March 15, 2017 Assets noted in Instance One started logging successfully to [REDACTED]

Mitigating Activities:

Description of Mitigating Activities:
 Mitigating Activities and Preventative Measure: [REDACTED] has enabled logging for all assets belonging to all the affected business units (Extent of condition is checked). No other assets other than noted in this self report were found with this condition.

- [REDACTED] generated test failed login attempts to confirm that relevant logs and alerts are generated and sent to the appropriate contacts.
- [REDACTED] has corrected all firewall and routing misconfigurations to ensure that alerts are appropriately routed and delivered to the intended recipients.
- [REDACTED] has established a defined location ([REDACTED]) for storing collected logs, a move that prevents logged incidents from being stored at a location different from where it was intended.
- Logging command is re-enabled on [REDACTED] networking devices.

Preventive Measures:
 Update [REDACTED] to enable future logging requests to be managed using the change control process. As a result, all aspects of the work order would be completely and accurately performed, and formally documented for future reference purposes. Target Date: July 14, 2017.
 [REDACTED] to update the [REDACTED] to include a responsibility for all [REDACTED] analysts to generate a quarterly report of all monitored NERC Assets. Update will also require all SMEs to review the generated report on a quarterly basis. This task will be added to [REDACTED] [REDACTED] for effective implementation and monitoring. This control will ensure logging and monitoring requests made by asset owners aligns with assets monitored by the [REDACTED] group. Target Date: May 25, 2017
 In order to prevent the re-occurrence of logging disabled on networking equipment [REDACTED] has implemented a peer check review in the procedure.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe
Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: The potential impact of this violation if exploited, is noted to be High VSL because failure to log or monitor security events could allow an internal or external threat to carry out malicious activities undetected. It could also lead to a denial of service if any of the cyber assets is compromised.
 The actual impact to the BPS is deemed to be Lower VSL because the vulnerability posed by this violation was not exploited. In addition, the availability of the services that relied on the affected assets was not impacted at any time during this violation or immediately afterwards.

Self Report

Risk Assessment of Impact to BPS: The risk posed by this violation to the BPS was assessed to be low based on the premise that the BPS did not record any service disruption as a result of the reported violations. Also, all identified mitigation activities has been either completed or affected assets removed from operation.

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
RFC2017017548	CIP-007-6 R4.	

Mitigation Plan Submitted On: [REDACTED]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: July 12, 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		
RFC2017017548	05/03/2017	CIP-007-6 R4.

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 R4 – Security Event Monitoring.

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

Following a scheduled QA assessment, performed by [REDACTED] early March 2017, it was noted that cyber assets belonging to three [REDACTED] Business Units: [REDACTED], [REDACTED], and [REDACTED] were not monitored for security incidents, logged (centrally, using [REDACTED] or locally), and sending out alerts to appropriate individuals when necessary. Also, logs were not kept for 90 days as required in CIP007-6 R4.3. Also, some business units did not receive alerts from the [REDACTED] team responsible for configuring and monitoring the affected assets.

Instance one: At the [REDACTED] it was discovered that [REDACTED] Servers, categorized as BCAs, managing the VM environment, were configured to capture security logs as per R4.1. Yet, the assets were not appropriately configured to send alerts to correct units and personnel. This therefore, constitutes a violation of CIP007-6 R4.2. In addition, logs were not kept for 90 days as required in CIP007-6 R4.3.

Alerts were not sent because incorrect protocols were used during configuration and the firewalls were misconfigured. As a result, security alerts generated from these assets were routed to the wrong recipients and storage. Another reason attributed to this violation is that [REDACTED] (Legacy) server and [REDACTED] (New) were both used in parallel, with different asset naming conventions. This situation led to a mismatch of asset IDs during configuration that further compounded the problem.

As of March 13, 2017, all the configuration and protocol errors are correct and the assets are configured to send alerts to the appropriate units and recipients. A trial alert was successfully generated on March 15 for a failed login attempt. The trial confirms that the mitigation effort is effective.

Instance two: [REDACTED] identified [REDACTED] servers capable of local logging only, were not manually reviewed every 15 calendar days as required. This situation is a violation of CIP-007 R4.4. These assets are now decommissioned and require no further corrective action. [REDACTED] were decommissioned on 3/17/17 using Change Order26373 and were removed from CIP002 list on 3/27/2017.

Instance three: In July 2016, a senior engineer with the [REDACTED] unit sent [REDACTED] of assets that needed to be monitored for security incidents to the [REDACTED] team. It was discovered that while other assets are logged, no log existed for [REDACTED] assets at [REDACTED]. Upon further investigation conducted by the senior network engineer, it was noted that the vendor [REDACTED] left a command on the devices since their inception, that turned logging off. The logging function was never turned back on; as a result, logs were not being generated from July 1st 2017 when the facility came into compliance till the discovery was made and fixed on January 12, 2017. Upon this discovery, the senior engineer notified [REDACTED] on January 25, 2017 of the failure. As a result, the assets were not monitored, nor were alerts generated for security events as required in CIP007-6 R4.2. This command was corrected to initiate logging.

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

- Instance 1: Verification procedure to ensure functionality was not in place which led to logs being routed to the wrong locations.
- Instance 2: The root cause of this violation at the [REDACTED] unit is attributed to a gap in the [REDACTED] monitoring process that did not provide business units with adequate insight into monitoring activities performed.
- Instance 3: The vendor [REDACTED] disabled the logging in order to execute the troubleshooting however after the task was completed the vendor did not switch on the logging back to its original configuration.

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

How was the violation discovered?

Instance One and Two: This possible violation was discovered during a routine QA assessment performed by [REDACTED] that began in January 2017.

Instance Three: This possible violation was discovered when the [REDACTED] team made an ad hoc confirmation inquiry to a [REDACTED] Analyst in December 2016, regarding the status of their assets being logged and monitored by the [REDACTED] group. He was told that no log was available for the [REDACTED] BCA assets involved in question.

Plan Details

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

Milestone 1: The intent outcome is to correct all firewall and routing misconfigurations regarding predefined systems and security incident logs. This will be measured through a quarterly [REDACTED] report. The evidence shows the firewall will allow [REDACTED] to pass through.

Milestone 2: The intent outcome to store logs for the [REDACTED] assets at [REDACTED]. This will be [REDACTED] through a quarterly [REDACTED] report. The evidence shows [REDACTED] event report for 12 [REDACTED] servers at [REDACTED].

Milestone 3: The intent outcome to confirm function of failed logins rule. This will be sustained through a quarterly [REDACTED] report. The evidence shows the generated failed login attempts to confirm that relevant logs and alerts are indeed generated and sent to the appropriate contacts.

Milestone 4: The intent outcome Update the [REDACTED] to include responsibilities for [REDACTED] SMEs to review for accuracy and completeness of [REDACTED] reported monitored assets every quarter.

Milestone 5: The intend outcome that [REDACTED] team should be able to see [REDACTED] from all our assets. This can be sustained or measured in regular basis by adding the spot check for logging between [REDACTED] and [REDACTED] team in [REDACTED] schedule. The evidence shows an updated [REDACTED] and [REDACTED] [REDACTED] stating that all [REDACTED] of the NERC assets need to be sent out to [REDACTED] personnel to verify that they receive [REDACTED] from the router and switches.

Milestone 6: The intent outcome to compare assets getting events to [REDACTED] and BCS list. The evidence will show the work done to complete that task.

Milestone 7: The intent outcome to us the change control process to document the future reference purposed. The evidence will show the enhanced [REDACTED] to define a process for verifying logging configurations after implementation to confirm intended outcomes are achieved.

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 12, 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
Correct all firewall and routing misconfigurations	Correct all firewall and routing misconfigurations regarding predefined systems and security incident logs.	03/13/2017	03/13/2017		No
Establish a clear	Establish a clear	03/13/2017	03/13/2017		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
location	location for storing collected logs.				
Generate failed login attempts	Generate failed login attempts to confirm that relevant logs and alerts are indeed generated and sent to the appropriate contacts.	03/15/2017	04/05/2017		No
Update Cyber Router and [REDACTED]	Update the [REDACTED] and [REDACTED] procedure to stat that all [REDACTED] of the NERC Assets need to be sent out to [REDACTED] personnel to verify that they receive [REDACTED] from the router	05/20/2017	04/28/2017		No
Update [REDACTED]	Update [REDACTED] to include responsibilities for [REDACTED] SMEs to review for accuracy and completeness of [REDACTED] reported monitored assets every quarter.	05/20/2017	04/28/2017		No
Extent of Condition	Review assets getting events to [REDACTED] and match that with BCS list.	06/30/2017			No
Enhance Process	Enhance [REDACTED] to define a process for verifying logging configurations after implementation to confirm intended outcomes are achieved.	07/12/2017			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 of this violation if exploited, is noted to be High VSL because failure to log or monitor security events could allow an internal or external threat to carry out malicious activities undetected.

The actual impact to the BPS is deemed to be Lower VSL because the vulnerability posed by this violation was not exploited. In addition, the availability of the services that relied on the affected assets was not impacted at any time during this violation or immediately afterwards.

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 enable future logging requests to be managed using the change control process. As a result, all aspects of the work order would be completely and accurately performed, and formally documented for future reference purposes. [REDACTED] to update the [REDACTED] [REDACTED] to include a responsibility for all [REDACTED] analysts to generate a quarterly report of all monitored NERC Assets. Update will also require all SMEs to review the generated report on a quarterly basis. This task will be added to [REDACTED] [REDACTED] for effective implementation and monitoring. This control will ensure logging and monitoring requests made by asset owners aligns with assets monitored by the [REDACTED] group. In order to prevent the re-occurrence of logging disabled on networking equipment.

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

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): RFC2017017548

Mitigated Standard Requirement(s): CIP-007-6 R4.

Scheduled Completion as per Accepted Mitigation Plan: July 12, 2017

Date Mitigation Plan completed: July 12, 2017

RF Notified of Completion on Date: [REDACTED]

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017017548 Certification Package.zip	File "RFC2017017548 Certification Package.zip" contains the cover page for the package and supporting documentation for all the milestones.	5,042,106

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 RFC2017017548

Standard/Requirement: CIP-007-6 R4

NERC Mitigation Plan ID: RFCMIT012983

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	Mitigation Plan Submittal	RF Acceptance	NERC Approval	Certification Submittal	Date of Completion
██████████	██████████	██████████		██████████	07/12/17

Description of Issue

Following a scheduled QA assessment performed in March 2017, it was noted that cyber assets belonging to three █████ Business Units were not monitored for security incidents, logged (centrally, using █████ or locally), and sending out alerts to appropriate individuals when necessary. Also, logs were not kept for 90 days as required in CIP007-6 R4.3. Also, the business units did not receive alerts from the ████████████████████ (██████) team responsible for configuring and monitoring the affected assets.

For the first instance, a verification procedure to ensure functionality was not in place which led to logs being routed to the wrong locations.

For the second instance, the root cause of this violation is attributed to a gap in the █████ monitoring process that did not provide business units with adequate insight into monitoring activities performed.

For the third instance, the vendor (██████) disabled the logging in order to execute the troubleshooting. However, after the task was completed the vendor did not switch on the logging back to its original configuration.

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	RFC2017017548 Certification Package	CIP-007-6 R4

Verification of Mitigation Plan Completion

Milestone 1: Correct all firewall and routing misconfigurations

File 1, “RFC2017017548 Certification Package”, Milestone 1 – Submit. This file shows the [REDACTED] setting being checked to allow the [REDACTED] to pass through the firewall. [REDACTED]. This setting was changed on [REDACTED] Firewalls.

Milestone # 1 Completion verified.

Milestone 2: Establish a clear location

File 1, “RFC2017017548 Certification Package”, Milestone 2 – Submit. This is a [REDACTED] report that shows the [REDACTED] servers save their [REDACTED] to [REDACTED] is the storage local for the logs from the [REDACTED] servers.

This file also has an example of a failed logon alert for [REDACTED] the [REDACTED] servers. The alert is dated April 27, 2017.

Milestone # 2 Completion verified.

Milestone 3: Generate failed login attempts

File 1, “RFC2017017548 Certification Package”, Milestone 3 - Submit.

Same evidence as Milestone 2.

This file also has an example of a failed logon alert for [REDACTED] [REDACTED] servers. The alert is dated April 27, 2017.

Milestone # 3 Completion verified.

Milestone 4: Update [REDACTED] and [REDACTED]

File 1, “RFC2017017548 Certification Package”, Milestone 4 - Submit. [REDACTED]
Router Configuration Management, ver 1.2, dated April 28, 2017.

This is the document that describes how the [REDACTED] routers should be configured.

Section 6.5 Logging (Page 5), a paragraph was added stating that [REDACTED] will send all of the [REDACTED] from their routers to the [REDACTED] personnel to verify they are receiving [REDACTED] from those routers. The [REDACTED] personnel confirms via email.

Milestone # 4 Completion verified.

Milestone 5: Update [REDACTED]

File 1, “RFC2017017548 Certification Package”, Milestone 5 - Submit. Cyber Security Monitoring, ver 4.8, dated April 28, 2017.

This is [REDACTED] program to monitor Critical Cyber Assets.

Under the Roles and Responsibility section (Page 6), [REDACTED] added the bullet point for the quarterly review asset monitoring report. The [REDACTED] is responsible for generating the report that confirms the SME's assets are sending logs to the [REDACTED]

Milestone # 5 Completion verified.

Milestone 6: Extent of Condition

File 1, “RFC2017017548 Certification Package”, Milestone 6 - Submit. [REDACTED] BES Cyber Systems List, print date July 5, 2016.

Page 2, this is a BES Cyber System List that [REDACTED] highlighted the BES Cyber Systems/Assets that are logged by [REDACTED] ([REDACTED])

Page 4, this is a list of Decommissioned BES Cyber Assets.

Page 5, this is a BES Cyber System List that shows which BES Cyber Systems/Assets that does not having logging capabilities.

Page 12, these are the email responses from each [REDACTED] areas verifying all BES Cyber Assets appears on the [REDACTED] report.

Milestone # 6 Completion verified.

Milestone 7k: Enhance [REDACTED] Process

File 1, “RFC2017017548 Certification Package”, Milestone 7 - Submit. [REDACTED]
[REDACTED] ver 3.2, dated June 13, 2017.

This is the [REDACTED] process to manage configuration changes.

Section 6.3 Execute Change Order Process (Page 6), a bullet item stated 'setting up/enabling or changing logging' was added.

Page 32, Task 74 was added to checklist for logging for new cyber assets.

Page 42. Task 126 was added to checklist for logging of changed assets.

Milestone # 7 Completion verified.

The Mitigation Plan is hereby verified complete.

Date: [REDACTED]

A handwritten signature in black ink, appearing to read "Tony Purgar". The signature is stylized with large, flowing loops.

Tony Purgar

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

Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [REDACTED] ([REDACTED])

NERC ID: [REDACTED]

Standard: CIP-007-6

Requirement: CIP-007-6 R4.

Date Submitted: March 26, 2018

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED] [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: September 15, 2017

Changed to December 19, 2017

End/Expected End Date:

Reliability Functions: [REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]

Is Possible Violation still No
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Date violation was contained:

Cause of Possible Violation: For [REDACTED], logs were being sent back to [REDACTED] on 2/16/2018, hence alerting started.

For [REDACTED], logs were being sent to [REDACTED] on 3/20/2018, hence alerting started.

Detailed Description:

Current Practice: [REDACTED] has a [REDACTED] in place to verify NERC Cyber Assets are being logged and alerted upon per CIP007 R4 P4.1 and P4.2. The program requires that logging of security events is enabled on each Cyber Asset per its capability. Assets with [REDACTED] or [REDACTED] operating systems are configured with an agent to send logs to the [REDACTED] log aggregator which are then forwarded to the [REDACTED] ([REDACTED] [REDACTED] use [REDACTED] to performing the function of [REDACTED] with use of [REDACTED] ([REDACTED] Server. Assets which cannot send logs to [REDACTED] are configured to send logs to a [REDACTED] server and then to [REDACTED] is configured to alert upon detection of anomalies for all assets and also upon disconnects. A quarterly report is generated from [REDACTED] that lists all the assets that are logging. This report is tracked in [REDACTED] [REDACTED] and is reviewed by SMEs to verify that all the assets are logging as per the requirement.

If the logging stops, the [REDACTED] ([REDACTED] [REDACTED])

Self Report

administrators receive an alert and began working with the asset's subject matter expert (SME) to resolve the issue.

Incident Description: In the current self-report regarding a possible noncompliance (PNC), two assets were not logging as per details below:

Asset ID [REDACTED]: The [REDACTED] administrator, identified a [REDACTED] cyber asset (ID [REDACTED]), a protected cyber asset (PCA), an Engineering WorkStation, that had a health monitoring configuration not set properly. Since these configurations were not set properly, there were no flags set to trigger an alert, even though alerting was always active. Therefore, no offenses was generated upon disconnect with the [REDACTED]. The asset stop communicating with the [REDACTED] on December 19, 2017. This PNC was reported on February 16, 2018.

Based on [REDACTED] and [REDACTED] improper configurations applied by the [REDACTED] [REDACTED] team did not alert support staff.

Asset ID [REDACTED]: In addition, while executing extent of condition during investigation of the above noted incident, the [REDACTED] administrator identified a [REDACTED] cyber asset (ID [REDACTED]), a Physical Access Control System (PACS) Workstation, that had stopped communicating with the [REDACTED]. This disconnect triggered a [REDACTED] offense. This offense was not immediately brought to the asset's SME attention. The following month, [REDACTED] had numerous recorded offensives on a single day, which resulted in the [REDACTED] administrator contacting the asset's SME to address. The asset's SME found service to be running and did not know that logs were not being sent to [REDACTED]. This PNC was reported on March 9, 2018. The asset stop communicating with the [REDACTED] on September 15, 2017.

Based on [REDACTED] and [REDACTED] offense was created, but due to lack of a formal process to contact SME and staff augmentation in [REDACTED], resulted in lack of follow up to address the disconnect.

During investigation of two assets, it was verified that last 90 days of logs where collected locally at the assets during the time frame when they were not communicating with [REDACTED]. Since both assets were identified as not sending logs to [REDACTED] a cursory review can only be done on last 90 days, as logs prior to that are set to be purged locally if they are over 90 days in age. Further, [REDACTED] reviewed the baseline of these two assets from September 2017 through March 2018, and did not find any unauthorized changes.

[REDACTED] verified that other than [REDACTED] monitoring, these two assets are compliant with every CIP requirement as per the categorization i.e. PCA.

What is the problem?

For asset [REDACTED], Improper configurations on agent did not alert [REDACTED] of log failure when an asset stopped communicating with the [REDACTED] which is a possible noncompliance of NERC CIP-007-6 R4.2.2.

For asset [REDACTED] incomplete troubleshooting and escalation step in the [REDACTED] monitoring and response process caused this asset to remain in a disconnected state with [REDACTED] which would result in possible noncompliance with NERC CIP-007-6 4.2 & 4.4.

Both assets are configured to send logs to the [REDACTED] and since logs were not being sent to [REDACTED] alerting failed.

Root Cause of Possible Violation:

As per the [REDACTED] & [REDACTED] performed on 3/13/2018 regarding asset [REDACTED], the health monitoring configuration settings within [REDACTED] were not applied properly. With current version of [REDACTED] this configuration is applied manually to each asset and that is due to [REDACTED] capability limitations. This one asset was missed due to manual effort when applying the configuration setting.

As per the [REDACTED] & [REDACTED] performed on 3/15/2018 regarding asset [REDACTED], An asset stopped sending logs to [REDACTED] which initiated an alert that was not responded to in a timely manner by [REDACTED] administrator. In addition, once [REDACTED]

Self Report

Preventative Measures:

- Modify the current [REDACTED] process maps for appropriate activity on disconnect, with a [REDACTED] agreement ([REDACTED] for disconnects by use of service desk ticket for all NERC asset offensives recorded in [REDACTED]. This will ensure a positive hand over between [REDACTED] administrator and SME. This will also reduce oversight of alert by [REDACTED] administrator and the SME, in which tracking of when asset communication with [REDACTED] had been restored.
- Modify and publish test template to all SME by using [REDACTED] Consulting email account, that address any change done to NERC assets to ensure verification of connection to [REDACTED] is running properly by executing a [REDACTED] connectivity check.
- Modify frequency of [REDACTED] report from quarterly to monthly. Have the report delivered on the third day of each month and have it include the previous month's day-to-day activity. That would highlight, if any disconnect with the [REDACTED] happened throughout the previous month.
- Since current version of [REDACTED] software does not allow the health monitoring configuration settings to be applied automatically on a cyber asset, create a process to include a documented cadence to move from an ad hoc review of [REDACTED] console to a formal process.
- Create an onboarding process for all SMEs, that would include instruction set for [REDACTED] related activities.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe

Actual Impact to BPS: Minimal

Description of Potential and Potential Impact:

Actual Impact to BPS: If security event occurred on a cyber security asset that had logging/alerting disabled, the impact would be considered high as support staff may be unaware of compromise. In addition, [REDACTED] logs contain BES Cyber Security Information that could be used to compromise Cyber Asset.

Actual Impact:

The impact of not logging/alerting from devices would be minimal because;
- Assets are in Physical Security Perimeter (PSP)
- Cyber controls such as antivirus monitoring and change management are in place.

Risk Assessment of Impact to BPS: Determination of High was made by referring to violation severity levels for CIP-007-6 R4 that state that the responsible entity has documented one or more process to identify undetected cyber security incidents by reviewing an entity to review logs every 15 calendar days but had missed two or more intervals.

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
RFC2018019469	CIP-007-6 R4.	

Mitigation Plan Submitted On: April 09, 2018

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: May 02, 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		
RFC2018019469	09/15/2017	CIP-007-6 R4.

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 R4 – Security Event Monitoring.

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

Current Practice: [REDACTED] has a [REDACTED] in place to verify NERC Cyber Assets are being logged and alerted upon per CIP007 R4 P4.1 and P4.2. The program requires that logging of security events is enabled on each Cyber Asset per its capability. Assets with [REDACTED] or [REDACTED] operating systems are configured with an agent to send logs to the [REDACTED] log aggregator which are then forwarded to the [REDACTED] [REDACTED] use [REDACTED] to performing the function of [REDACTED] with use of [REDACTED] Server. Assets which cannot send logs to [REDACTED] are configured to send logs to a [REDACTED] server and then to [REDACTED] is configured to alert upon detection of anomalies for all assets and also upon disconnects. A quarterly report is generated from [REDACTED] that lists all the assets that are logging. This report is tracked in [REDACTED] [REDACTED] and is reviewed by SMEs to verify that all the assets are logging as per the requirement. If the logging stops, the [REDACTED] [REDACTED] administrators receive an alert and began working with the asset's subject matter expert (SME) to resolve the issue.

Incident Description: In the current self-report regarding a possible noncompliance (PNC), two assets were not logging as per details below:

Asset ID [REDACTED]: The [REDACTED] administrator, identified a [REDACTED] cyber asset (ID [REDACTED]), a protected cyber asset (PCA), an Engineering WorkStation, that had a health monitoring configuration not set properly. Since these configurations were not set properly, there were no flags set to trigger an alert, even though alerting was always active. Therefore, no offenses was generated upon disconnect with the [REDACTED]. The asset stop communicating with the [REDACTED] on December 19, 2017. This PNC was reported on February 16, 2018.

Based on [REDACTED] and [REDACTED] improper configurations applied by the [REDACTED] [REDACTED] team did not alert support staff.

Asset [REDACTED]: In addition, while executing extent of condition during investigation of the above noted incident, the [REDACTED] administrator identified a [REDACTED] cyber asset ([REDACTED]), a Physical Access Control System (PACS) Workstation, that had stopped communicating with the [REDACTED]. This disconnect triggered a [REDACTED] offense. This offense was not immediately brought to the asset's SME attention. The following month, [REDACTED] had numerous recorded offensives on a single day, which resulted in the [REDACTED] administrator contacting the asset's SME to address.

The asset's SME found service to be running and did not know that logs were not being sent to [REDACTED]. This PNC was reported on March 9, 2018. The asset stop communicating with the [REDACTED] on September 15, 2017.

Based on [REDACTED] and [REDACTED] offense was created, but due to lack of a formal process to contact SME and staff augmentation in CSDS, resulted in lack of follow up to address the disconnect.

During investigation of two assets, it was verified that last 90 days of logs where collected locally at the assets during the time frame when they were not communicating with [REDACTED]. Since both assets were identified as not sending logs to [REDACTED] a cursory review can only be done on last 90 days, as logs prior to that are set to be purged locally if they are over 90 days in age. Further, [REDACTED] reviewed the baseline of these two assets from September 2017 through March 2018, and did not find any unauthorized changes. [REDACTED] verified that other than [REDACTED] monitoring, these two assets are compliant with every CIP requirement as per the categorization i.e. PCA.

What is the problem?

For asset [REDACTED], Improper configurations on agent did not alert [REDACTED] of log failure when an asset stopped communicating with the [REDACTED] which is a possible noncompliance of NERC CIP-007-6 R4.2.2.

For asset [REDACTED], incomplete troubleshooting and escalation step in the [REDACTED] monitoring and response process caused this asset to remain in a disconnected state with [REDACTED] which would result in possible noncompliance with NERC CIP-007-6 4.2 & 4.4.

Both assets are configured to send logs to the [REDACTED] and since logs were not being sent to [REDACTED] alerting failed.

Root Cause of Possible Violation:

As per the [REDACTED] & RCA performed on 3/13/2018 regarding asset [REDACTED], the health monitoring configuration settings within [REDACTED] were not applied properly. With current version of [REDACTED] this configuration is applied manually to each asset and that is due to [REDACTED] capability limitations. This one asset was missed due to manual effort when applying the configuration setting.

As per the [REDACTED] & RCA performed on 3/15/2018 regarding asset [REDACTED], An asset stopped sending logs to [REDACTED] which initiated an alert that was not responded to in a timely manner by [REDACTED] administrator. In addition, once [REDACTED] administrator had acknowledged the alert, there was no formal process described on how the [REDACTED] administrator should address and resolve the disconnect with the SME. As in this case, the issue was not followed through to verify communication had been restored.

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

The noncompliance is related to lack of formal process in the [REDACTED] documentation and due to manual configuration with regards to health configuration settings upon disconnect with the [REDACTED] server and communicating with the SME to resolve issue.

Timeline:

9/15/2017 - [REDACTED] Cyber security asset [REDACTED] stopped communicating with [REDACTED]

10/16/2017 - [REDACTED] administrator contacted asset's SME to inform that asset [REDACTED] was not sending logs to [REDACTED]

10/16/2017 - SME received email from incident [REDACTED] administrator and reviewed settings and confirmed that [REDACTED] service was running, but did not confirm connectivity to [REDACTED]

9/15/2017 - 3/20/2018 - Logs remain on the asset [REDACTED].

9/15/2017 - 3/20/2018 - The review of logs of asset [REDACTED] with in every 15 days has not been conducted, which is a violation of CIP R4.4.

12/19/2017 - Within 24 HOURS OF 12/19/2017 - A change on [REDACTED] Antivirus client for asset [REDACTED] was being conducted as per Change Order [REDACTED]. This change may have disabled the [REDACTED] client.

2/16/2018 - Ad-hoc review of [REDACTED] console by [REDACTED] administrator discovered that asset [REDACTED] was not sending logs to console & the [REDACTED] contacted SME to fix the issue.

2/16/2018 - Asset [REDACTED] connection was restored and logs were being sent to [REDACTED]

3/9/2018 - [REDACTED] ([REDACTED]) conducted.

3/9/2018 - While executing extent of condition during investigation of the above noted incident [REDACTED] administrator contacted the [REDACTED] to discuss possible noncompliance (PNC) for asset [REDACTED] since this asset had failed to communicate with the [REDACTED] and was not reported to the [REDACTED] earlier.

3/13/2018 - Root cause analysis (RCA) conducted for asset [REDACTED].

3/15/2018 - [REDACTED] and RCA conducted for asset [REDACTED].

3/20/2018 - Asset [REDACTED] connection was restored and logs were being sent to [REDACTED] per change order [REDACTED].

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

For asset [REDACTED], the violation was identified when [REDACTED] administrator did an ad hoc review of the [REDACTED] console, which had displayed that the asset had stopped communicating with the [REDACTED]

For asset [REDACTED], the violation was identified by [REDACTED] administrator while executing extent of condition during investigation of the above noted violation.

Plan Details

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

Milestone 1 - Modify and publish test template

Description: [REDACTED] uses a pre-specified test template to ensure that the security controls, including logging, are still working after a change is incorporated. In case of asset [REDACTED], asset SME applied patch and verified that the [REDACTED] client is running. However, tech never verified if the asset was sending logs to [REDACTED] server. A gap in the test template was determined that template is asking to verify if [REDACTED] client is running. This milestone will ensure SMEs are verifying connectivity of [REDACTED] is tested after every change to prevent prolonged disconnections.

Purpose: Purpose of this milestone is to modify the test template to cover how to verify the connectivity with [REDACTED] of any asset that was changed and to republish and communicate that test template to all SMEs using [REDACTED] Consulting email account.

Evidence:

- 1) Evidence will include the updated test template used for reference by the SMEs.
- 2) Evidence will include the email communication of the updated test template that was sent to every SME.

Milestone 2 - Check extent of condition

Description: Ensure that these two assets were the only assets not being appropriately monitored.

Purpose: Purpose of this milestone is to check the extent of condition on the [REDACTED] console for all NERC assets monitored by the [REDACTED]

Evidence: Screenshot(s) that display activity that [REDACTED] [REDACTED] administrator completed to verify extent of condition (signed by [REDACTED] [REDACTED] administrator and date.)

Milestone 3 - Reconnection of Assets to [REDACTED]

Description: Ensure that two assets that stopped sending logs to [REDACTED] server, start sending logs again.

Purpose: Purpose of this milestone is to ensure that both assets (id [REDACTED] and [REDACTED]) are logging as of 02/16/2018 and 03/20/2018 respectively.

Evidence: The evidence will include a screenshot showing that the assets are communicating with [REDACTED] as of 2/16/2018 & 3/20/2018 respectively.

Milestone 4 - Assets store logs locally

Description: Ensure that two assets maintained logs locally at time of disconnect.

Purpose: Purpose of this milestone is to ensure that both assets stored logs locally, up to 90 days, until connection with [REDACTED] was reestablished.

Evidence: The evidence will include a screenshot showing that all available local logs for assets [REDACTED] have been exported to a shared location for the [REDACTED] [REDACTED] administrator.

Milestone 5 - Review of logs stored locally

Description: Ensure that these two assets local logs did not contain alerts/alarms that required attention.

Purpose: Purpose of this milestone is to conduct cursory review on both asset's local logs, that are available, to verify there were zero alerts that require further investigation during this time.

Evidence: The evidence will include an excel workbook that includes the [REDACTED] [REDACTED] administrators manual review of the logs from asset [REDACTED].

Milestone 6 - Modify [REDACTED] Process Maps

Description: Ensure process is in place to prevent miss-handling of [REDACTED] offensives.

Purpose: Purpose of this milestone is to modify the current [REDACTED] process maps for appropriate activity on disconnect, with a [REDACTED] agreement ([REDACTED] for disconnects by use of service desk ticket for all NERC asset offenses recorded in [REDACTED]. This will ensure a positive hand over between [REDACTED] [REDACTED] administrator and SME.

This will also reduce oversight of alert by [REDACTED] administrator and the SME, in tracking when asset communication with [REDACTED] had been restored.

Evidence:

- 1) Evidence will include an updated program that will have steps on how to handle a disconnect with SME.
- 2) Evidence will include an email from the manager of [REDACTED] to staff informing them of the updated program.

Milestone 7 - Modify frequency of [REDACTED] report

Description: Ensure all assets have been review for completeness to prevent prolonged disconnections.

Purpose: Purpose of this milestone is to modify the frequency of the [REDACTED] report from quarterly to monthly, to have the report delivered on the third day of each month, and to have it include the previous month's day-to-day activity. That would highlight whether any disconnect with the [REDACTED] had happened throughout the previous month.

Evidence:

- 1) Evidence will include an updated program to reflect that the monthly [REDACTED] report review is being sustained.
- 2) Evidence will include an email from the manager of [REDACTED] to staff informing them of the updated program.

Milestone 8 - Formalize ad hoc review cadence

Description: Ensure all assets have been reviewed for completeness to prevent prolonged disconnections.

Purpose: Since current version of [REDACTED] software does not allow the health monitoring configuration settings to be applied automatically on a cyber asset, the purpose of this milestone is to create a process to include a documented cadence to move from an ad hoc review of [REDACTED] console to a formal process.

Evidence:

- 1) Evidence will include the created process that will include a monthly review of [REDACTED] console and the health check configuration.
- 2) Evidence will include an email from the manager of [REDACTED] to staff informing them of the new process.

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 02, 2018

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

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Milestone 1 - Modify and publish test template	Description: Ensure SMEs are verifying connectivity to [REDACTED] is tested after every change to prevent prolonged disconnections. Evidence: 1) Evidence will include the updated test template used for reference by the	03/23/2018	03/23/2018		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
	SMEs. 2) Evidence will include the email communication of the updated test template that was sent to every SME.				
Milestone 2 - Check extent of condition	Description: Ensure that these two assets were the only assets not being appropriately monitored. Evidence: Screenshot(s) that display activity that [REDACTED] administrator completed to verify extent of condition (signed by [REDACTED] administrator and date.)	03/28/2018	03/27/2018		No
Milestone 3 - Reconnection of Assets to [REDACTED]	Description: Ensure that two assets that stopped sending logs to [REDACTED] server, start sending logs again. Evidence: The evidence will include a screenshot showing that the assets are communicating with [REDACTED] as of 2/16/2018 & 3/20/2018 respectively.	04/02/2018	04/02/2018		No
Milestone 4 - Assets store logs locally	Description: Ensure that two assets maintained	04/02/2018	04/02/2018		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
	<p>logs locally at time of disconnect. Evidence: The evidence will include a screenshot showing that all available local logs for assets [REDACTED] [REDACTED] have been exported to a shared location for the [REDACTED] [REDACTED] administrator.</p>				
Milestone 5 - Review of logs stored locally	<p>Description: Ensure that these two assets local logs did not contain alerts/alarms that required attention. Evidence: The evidence will include an excel workbook that includes the [REDACTED] [REDACTED] administrators manual review of the logs from asset [REDACTED].</p>	04/03/2018	04/02/2018		No
Milestone 6 - Modify [REDACTED] Process Maps	<p>Description: Ensure process is in place to prevent miss-handling of [REDACTED] offensives. Evidence: 1) Evidence will include an updated program that will have steps on how to handle a disconnect with SME. 2) Evidence will include an email from the manager of [REDACTED] to staff</p>	05/02/2018			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
	informing them of the updated program.				
Milestone 7 - Modify frequency of [REDACTED] report	Description: Ensure all assets have been review for completeness to prevent prolonged disconnections. Evidence: 1) Evidence will include an updated program to reflect that the monthly [REDACTED] report review is being [REDACTED] 2) Evidence will include an email from the manager of [REDACTED] to staff informing them of the updated program.	05/02/2018			No
Milestone 8 - Formalize ad hoc review cadence	Description: Ensure all assets have been reviewed for completeness to prevent prolonged disconnections. Evidence: 1) Evidence will include the created process that will include a monthly review of [REDACTED] console and the health check configuration. 2) Evidence will include an email from the manager of [REDACTED] to staff informing them of the new process.	05/02/2018			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.

Update of test template that was completed on 3/23 will minimize the risk of reoccurrence. In addition, [REDACTED] verified that all the assets except two reported in in this PNC were logging.

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 this mitigation plan, [REDACTED] will use the updated processes to minimize the probability of this type of noncompliance happening again and therefore reduce the risk of similar violations.

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

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): RFC2018019469

Mitigated Standard Requirement(s): CIP-007-6 R4.

Scheduled Completion as per Accepted Mitigation Plan: May 02, 2018

Date Mitigation Plan completed: May 02, 2018

RF Notified of Completion on Date: May 02, 2018

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2018019469 Certification Package.zip	File "RFC2018019469 Certification Package.zip" contains a coversheet for the package plus evidence to support completion of each milestone.	8,966,367

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 RFC2018019469

████████████████████ (██████████)

Standard/Requirement: CIP-007-6 R4

NERC Mitigation Plan ID: RFCMIT013708

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	Mitigation Plan Submittal	RF Acceptance	NERC Approval	Certification Submittal	Date of Completion
Self-Report 03/26/18	04/09/18	05/04/18	05/17/18	05/02/18	05/02/18

Description of Issue

Assets with ██████████ or ██████████ operating systems are configured with an agent to send logs to the ██████████ log aggregator which are then forwarded to the ██████████ (██████████ use ██████████ to perform the function of ██████████ with use of ██████████ ██████████ Server. Assets that cannot send logs to ██████████ are configured to send logs to a ██████████ server and then to ██████████ is configured to alert upon detection of anomalies for all assets and also upon disconnects. A quarterly report is generated from ██████████ that lists all the assets that are logging. This report is tracked in ██████████ ██████████ and is reviewed by SMEs to verify that all the assets are logging as per the requirement.

If the logging stops, the ██████████ (██████████ ██████████ administrators receive an alert and began working with the asset's subject matter expert (SME) to resolve the issue.

Two assets were not logging:

Asset ID ██████████: The ██████████ administrator, identified a ██████████ cyber asset (ID ██████████), a protected cyber asset (PCA), an Engineering WorkStation, that had a health monitoring configuration not set properly. Since these configurations were not set properly, there were no flags set to trigger an alert, even though alerting was always active. Therefore, no offenses were

generated upon disconnect with the [REDACTED]. The asset stop communicating with the [REDACTED] on December 19, 2017.

Asset ID [REDACTED]: In addition, the [REDACTED] administrator identified a [REDACTED] cyber asset (ID [REDACTED]), a Physical Access Control System (PACS) Workstation that had stopped communicating with the [REDACTED]. This disconnect triggered a [REDACTED] offense. This offense was not immediately brought to the asset's SME attention. The following month, [REDACTED] had numerous recorded offensives on a single day, which resulted in the [REDACTED] administrator contacting the asset's SME. The asset stopped communicating with the [REDACTED] on September 15, 2017.

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	RFC2018019469 Certification Package	CIP-007-6 R4

Verification of Mitigation Plan Completion

Milestone 1: Modify and publish test template.

Proposed Completion Date: March 23, 2018

Actual Completion Date: March 23, 2018

File 1, “RFC2018019469 Certification Package”, Milestone 1, Page 2, shows the updates made to the entities’ Baseline Changes and Security Controls Testing and Review documentation as indicated in this milestone. In this evidence, the entity added a section included testing for [REDACTED] and the [REDACTED] to ensure the SME verifies connectivity. In addition, this segment provides expected results and required actions if the outcome differs from the expected outcome. Page 3 shows the revision history of the above mentioned document showing the latest update of 3-20-2018 in order to incorporate the above mentioned changes. Pages 4 and 5 show the email communication to affected employees showing that the above mentioned changes were incorporated and to ensure that they know where the document is stored, they review the changes, ask questions if applicable, and the point of contact for these said changes.

Milestone # 1 Completion verified.

Milestone 2: Check extent of condition.

Proposed Completion Date: March 28, 2018

Actual Completion Date: March 27, 2018

File 1, “*RFC2018019469 Certification Package*”, milestone 2, Pages 2 through 14, show that the entities’ [REDACTED] (as part of the extent of condition review) was monitoring all required NERC devices as of 3-27-2018. Page 115 shows that the SME responsible for the review ensured that all assets from the above mentioned pages were checked to ensure that [REDACTED] [REDACTED] agents were installed on them, running as indicated, and that they were all reporting as required. In addition, the entities’ compliance manager (on a later date of 1-5-2018) requested that the SME signed the statement as an attestation to ensure the work was completed as stated. Page 16 shows that the entities’ internal QA team sampled the above tested devices to double check/peer review the above mentioned work for accuracy in which all of the 45 samples passed as previously indicated.

Milestone # 2 Completion verified.

Milestone 3: Reconnection of Assets to [REDACTED]

Proposed Completion Date: April 2, 2018

Actual Completion Date: April 2, 2018

File 1, “*RFC2018019469 Certification Package*”, milestone 3, Page 2, shows screenshots from [REDACTED] which indicate that the assets mentioned in the self-report (x2) were in fact sending logs to [REDACTED]

Milestone # 3 Completion verified.

Milestone 4: Assets store logs locally.

Proposed Completion Date: April 2, 2018

Actual Completion Date: April 2, 2018

File 1, “*RFC2018019469 Certification Package*”, milestone 4, Page 2 through 5, show that the available log for the above mentioned devices (x2) had been exported, illustrating that logs were being stored locally.

Milestone # 4 Completion verified.

Milestone 5: Review of logs stored locally.

Proposed Completion Date: April 3, 2018

Actual Completion Date: April 2, 2018

File 1, “RFC2018019469 Certification Package”, milestone 5, Pages 2 through 4, show that the SME manually reviewed the above mentioned device (x2) logs via an export to excel. Page 2 shows the results of the SME’s manual review and page 4 shows that the SME indicated that these devices (x2) passed the review.

Milestone # 5 Completion verified.

Milestone 6: Modify [REDACTED] Process Maps.

Proposed Completion Date: May 2, 2017

Actual Completion Date: May 2, 2017

File 1, “RFC2018019469 Certification Package”, milestone 6, Page 2, shows that the entity Compliance Manager sent out a notification (dated 4-27-2018) to the [REDACTED] Team ([REDACTED] indicating changes within the update to the [REDACTED] and where it is stored. Pages 3 and 4 show the [REDACTED] organizational chart and the acknowledgement that the members of that department read and understand the procedural update. Page 5, shows a screenshot of the link and the company intranet page showing where the above mentioned procedural updates can be found. Page 15 shows the update to the procedure as indicated by the previously mentioned email to the [REDACTED] Department. Page 21 shows the revision history table indicating that the changes were completed and made effective on April 16, 2018. Pages 23 through 37 show the previous procedure pre-modification.

Milestone # 6 Completion verified.

Milestone 7: Modify frequency of [REDACTED] report.

Proposed Completion Date: May 2, 2018

Actual Completion Date: May 2, 2018

File 1, “RFC2018019469 Certification Package”, milestone 7 Pages 2 through 37 show that the entities’ procedure was updated to reflect the frequency of the [REDACTED] report. File 1 RFC2018019469 Certification Package; milestone 2, Pages 2 through 14, show that the entities’ [REDACTED] (as part of the extent of condition review) was monitoring all required NERC devices as of March 27, 2018. Page 115 shows that the SME responsible for the review ensured that all assets from the above mentioned pages were checked to ensure that [REDACTED] agents were installed on them, running as indicated, and that they were all reporting as required.

Milestone # 7 Completion verified.

Milestone 8: Formalize ad hoc review cadence.

Proposed Completion Date: May 2, 2018

Actual Completion Date: May 2, 2018

File 1, “RFC2018019469 Certification Package”, milestone 6, Page 2, shows that the entity Compliance Manager sent out a notification (dated 4-27-2018) to the [REDACTED] Team ([REDACTED] indicating changes within the update to the [REDACTED] and where it is stored. Pages 3 and 4, show the [REDACTED] organizational chart and the acknowledgement that the members of that department have read and understand the procedural update. Page 5, shows a screenshot of the link and the company intranet page showing where the above mentioned procedural updates can be found. Page 15 shows the update to the procedure as indicated by the previously mentioned email to the [REDACTED] Department. Page 21 shows the revision history table indicating that the changes were completed and made effective on April 16, 2018. Pages 23 through 37 show the previous procedure pre-modification.

Milestone # 8 Completion verified.

The Mitigation Plan is hereby verified complete.

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

A handwritten signature in black ink, appearing to read 'Anthony Jablonski', with a long horizontal flourish extending to the right.

Date: July 5, 2018

Anthony Jablonski
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [REDACTED] ([REDACTED])

NERC ID: [REDACTED]

Standard: CIP-007-6

Requirement: CIP-007-6 R4.

Date Submitted: July 17, 2018

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED] [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: July 01, 2016

End/Expected End Date:

Reliability Functions: [REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]

Is Possible Violation still No
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Date violation was contained:
Cause of Possible Violation: Asset ID [REDACTED] logs were being sent to [REDACTED] on 6/25/2018, hence alerting and monitoring started.

Detailed Description:
Current Practice: [REDACTED] has a [REDACTED] in place to verify NERC Cyber Assets are being logged and alerted upon per CIP007 R4 P4.1 and P4.2. The program requires that logging of security events is enabled on each Cyber Asset per its capability. Assets with [REDACTED] or [REDACTED] operating systems are configured with an agent to send logs to the [REDACTED] [REDACTED] log aggregator, which are then forwarded to the [REDACTED] [REDACTED] [REDACTED] uses [REDACTED] to perform the function of [REDACTED] along with the [REDACTED] servers. Assets which cannot send logs to [REDACTED] are configured to send logs to a [REDACTED] server and then to [REDACTED] is configured to alert upon detection of anomalies for all assets and also upon disconnects. A monthly report is generated from [REDACTED] that lists all the assets that are logging. This report is tracked in [REDACTED] [REDACTED] and is reviewed by SMEs to verify that all the assets are logging as per the requirement.
If the logging stops, the [REDACTED] [REDACTED] administrators receive an alert and began working with the asset's subject matter expert (SME) to resolve the issue.
If during review of the monthly report an anomaly and/or difference is found,

Self Report

the SME attempts to resolve the issue and if necessary contacts the [REDACTED] administrator for assistance.

Incident Description: In the current self-report regarding a possible noncompliance (PNC), a [REDACTED] asset was found to not have been sending logs to [REDACTED] for proper monitoring and alerting. The subject matter expert (SME) when reviewing the monthly [REDACTED] report for the month of June, 2018, identified a [REDACTED] cyber asset (ID [REDACTED]), a protected cyber asset (PCA), an engineering workstation, that was not listed on the report. This PNC was reported on June 20, 2018. Through research by [REDACTED] administrators, it was unable to be determined if [REDACTED] had ever received logs for this asset and that this asset had an old cert file (year 2008) configured.

It was also determined that the recent self-report, that was reported and mitigated (RFC2018019469), had an inaccurate/incomplete extent of condition check. This extent of condition should have included an assignment to all NERC asset subject matter experts (SME), to verify that all their assets logs were indeed being monitored by [REDACTED] or documented by other means. Further, since security event logs are set to store locally on this asset, CIP 007 requirement 4.1 & 4.3 are not in violation. This violation relates to CIP 007 requirement 4.2, in which generated alerts, for security events, per the asset's capability, are not alerting.

Based on [REDACTED] ([REDACTED]) and the understanding that [REDACTED] has had increase in self-reports related to this NERC CIP 7 Requirement 4, that a deeper dive into both root cause and the extent of condition will be necessary. [REDACTED] will use utilize a systematic problem solving process (A3) to attempt to stop future violations with this requirement.

What is the problem?

For asset [REDACTED], improper cert file was installed, which prevented asset's logs from being sent to [REDACTED] for monitoring and alerting which is a possible noncompliance of NERC CIP-007 R4.2.

Root Cause of Possible Violation:

Based on [REDACTED] ([REDACTED]) and the understanding that [REDACTED] has had increase in self-reports related to this NERC CIP 7 Requirement 4, that a deeper dive into both root cause and the extent of condition will be necessary. [REDACTED] will utilize a systematic problem solving process (A3) to attempt to stop future violations with this requirement.

Mitigation Plan will include the root cause.

How was the violation discovered?

[REDACTED] have a monthly control that [REDACTED] ([REDACTED]) lists all the assets that are reporting to [REDACTED] and have SMEs review it. This review is tracked using [REDACTED]. For asset [REDACTED], the violation was identified by the subject matter expert (SME) when performing a review of the [REDACTED] monthly report, which had identified that the asset was not being monitored by [REDACTED].

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

This noncompliance is related to lack of formal process in the [REDACTED] documentation to check for old cert files and prescribe process to verify all [REDACTED] NERC assets that are capable having logs monitored by [REDACTED] are being monitored.

Timeline:

7/1/2016 - NECR CIP Version 6 was implemented, and therefore, capable assets were configured for alerting via [REDACTED]

6/14/2018 - The [REDACTED] SME, while conducting review of the monthly [REDACTED] report provided by the [REDACTED] found that Medium Cyber Security Asset [REDACTED] was not a part of population.

6/20/2018 - [REDACTED] SME self-reported a possible noncompliance (PNC) to the [REDACTED]

Self Report

6/25/2018 - [REDACTED] SME, while investigating, determined that the asset [REDACTED] certification file (cert) for the [REDACTED] agent was old and out of date (year 2008), which was the reason this asset logs were not being monitored by [REDACTED]

6/25/2018 - [REDACTED] SME updated the cert on the asset [REDACTED] and after the update, found the asset to be connected to [REDACTED] successfully.

6/25/2018 - [REDACTED] performed an extent of condition check by making sure all assets that were checking in with [REDACTED] are in a healthy state.

6/27/2018 - [REDACTED] QA conducted an [REDACTED] ([REDACTED])

7/5/2018 - A3 had a kick off meeting.

Mitigating Activities:

Description of Mitigating Immediate Correcting Activities:
 Activities and Preventative • Asset [REDACTED] had correct cert installed and is sending logs to [REDACTED] as of
 Measure: 6/25/2018.

Mitigating Activities:
 • To be determined from A3 problem solving session has concluded.

Preventative Measures:
 • To be determined from A3 problem solving session has concluded.

Date Mitigating Activities
 Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe
 Actual Impact to BPS: Minimal

Description of Potential and Potential Impact: If security event occurred on a cyber security asset that had
 Actual Impact to BPS: logging/alerting disabled, the impact would be considered high as support staff
 may be unaware of compromise. In addition, [REDACTED] logs contain BES Cyber
 Security Information that could be used to compromise Cyber Asset.

Actual Impact: The impact of not logging/alerting from devices would be minimal because;
 - Assets are in Physical Security Perimeter (PSP)
 - Cyber controls such as patching, baseline monitoring, antivirus monitoring, and change management are in place.

Risk Assessment of Impact to BPS: Determination of High was made because of repeat issue and also by referring to violation severity levels for CIP-007-6 R4 that state that the responsible entity has documented one or more process to identify undetected cyber security incidents by reviewing an entity to review logs every 15 calendar days but had missed two or more intervals.

Additional Entity Comments:

Self Report

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [REDACTED]

Mitigation Plan Code: RFCMIT014196

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2018020086	CIP-007-6 R4.	

Mitigation Plan Submitted On: October 12, 2018

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: December 21, 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] [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		
RFC2018020086	07/01/2016	CIP-007-6 R4.
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 R4 – Security Event Monitoring.		

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

Current Practice: [REDACTED] has a [REDACTED] in place to verify NERC Cyber Assets are being logged and alerted upon per CIP007 R4 P4.1 and P4.2. The program requires that logging of security events is enabled on each Cyber Asset per its capability. Assets with [REDACTED] or [REDACTED] operating systems are configured with an agent to send logs to the [REDACTED] ([REDACTED] log aggregator, which are then forwarded to the [REDACTED] ([REDACTED] uses [REDACTED] to perform the function of [REDACTED] along with the [REDACTED] servers. Assets which cannot send logs to [REDACTED] are configured to send logs to a [REDACTED] server and then to [REDACTED] is configured to alert upon detection of anomalies for all assets and also upon disconnects. A monthly report is generated from [REDACTED] that lists all the assets that are logging. This report is tracked in [REDACTED] [REDACTED] and is reviewed by SMEs to verify that all the assets are logging as per the requirement.

If the logging stops, the [REDACTED] ([REDACTED] [REDACTED] administrators receive an alert and began working with the asset's subject matter expert (SME) to resolve the issue.

If during review of the monthly report an anomaly and/or difference is found, the SME attempts to resolve the issue and if necessary contacts the [REDACTED] [REDACTED] administrator for assistance.

Incident Description: In the current self-report regarding a possible noncompliance (PNC), a [REDACTED] asset was found to not have been sending logs to [REDACTED] for proper monitoring and alerting. The subject matter expert (SME) when reviewing the monthly [REDACTED] report for the month of June, 2018, identified a [REDACTED] cyber asset (ID [REDACTED]), a protected cyber asset (PCA), an engineering workstation, that was not listed on the report. This PNC was reported on June 20, 2018. Through research by [REDACTED] administrators, it was unable to be determined if [REDACTED] had ever received logs for this asset and that this asset had an old cert file (year 2008) configured.

It was also determined that the recent self-report, that was reported and mitigated (RFC2018019469), had an inaccurate/incomplete extent of condition check. This extent of condition should have included an assignment to all NERC asset subject matter experts (SME), to verify that all their assets logs were indeed being monitored by [REDACTED] or documented by other means.

Further, since security event logs are set to store locally on this asset, CIP 007 requirement 4.1 & 4.3 are not in violation. This violation relates to CIP 007 requirement 4.2, in which generated alerts, for security events, per the asset's capability, are not alerting.

Based on [REDACTED] ([REDACTED] and the understanding that [REDACTED] has had increase in self-reports related to this NERC CIP 7 Requirement 4, that a deeper dive into both root cause and the extent of condition will be necessary. [REDACTED] will use utilize a systematic problem solving process (A3) to attempt to stop future violations with this requirement.

Results from the A3 have found that the NERC CIP [REDACTED] Program, did not contain a detailed prescribed process for SME to follow when onboarding and maintaining an asset as it relates to centralized logging and alerting.

What is the problem?

For asset [REDACTED], improper cert file was installed, which prevented asset's logs from being sent to [REDACTED] for monitoring and alerting which is a possible noncompliance of NERC CIP-007 R4.2.

Root Cause of Possible Violation:

A3 concluded that the root cause is the current asset verification process is too high-level, hence does not instruct SME to capture the verification that was done for all assets that can send logs to the [REDACTED] server ([REDACTED]) where indeed sending logs to the [REDACTED] Server.

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

This noncompliance is related to lack of formal process in the NERC CIP [REDACTED] Program documentation to prescribe a process to verify all [REDACTED] NERC assets that are capable having logs monitored by [REDACTED] are being monitored.

Timeline:

7/1/2016 - NECR CIP Version 6 was implemented, and therefore, capable assets were configured for alerting via [REDACTED]

6/14/2018 - The [REDACTED] SME, while conducting review of the monthly [REDACTED] report provided by the [REDACTED] found that Medium Cyber Security Asset [REDACTED] was not a part of population.

6/20/2018 - [REDACTED] SME self-reported a possible noncompliance (PNC) to the [REDACTED]

6/25/2018 - [REDACTED] SME, while investigating, determined that the asset [REDACTED] certification file (cert) for the [REDACTED] agent was old and out of date (year 2008), which was the reason this asset logs were not being monitored by [REDACTED]

6/25/2018 - [REDACTED] SME updated the cert on the asset [REDACTED] and after the update, found the asset to be connected to [REDACTED] successfully.

6/25/2018 - [REDACTED] performed an extent of condition check by making sure all assets that were checking in with [REDACTED] are in a healthy state.

6/27/2018 - [REDACTED] conducted an [REDACTED] ([REDACTED])

7/5/2018 - A3 had a kick off meeting.

9/10/2018 - A3 discovered root cause and counter measures

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

The violation was identified when the SME reviewed the monthly report and found that the logs of asset [REDACTED] were not being captured and monitored by the [REDACTED] solution.

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 - Asset [REDACTED] logs are monitored by [REDACTED] server

Description: Ensure that asset has correct cert file installed and the asset's logs begin being monitored by [REDACTED] server.

Purpose: Purpose of this milestone is to ensure that the asset [REDACTED] has correct cert file installed and that asset [REDACTED] logs are being monitored by [REDACTED] server as of 06/25/2018.

Evidence:

- 1) The evidence will include description of how cert was updated on asset [REDACTED] on 6/25/2018.
- 2) The evidence will include a screenshot displaying asset [REDACTED] contains new cert.
- 3) The evidence will include a screenshot displaying timeline that asset [REDACTED] logs are being captured by [REDACTED]

Milestone 2 - SME check for extent of condition

Description: In use of the [REDACTED] [REDACTED] each SMEs will conduct review of assets and verify that each asset, which can send logs is configured and being monitored by [REDACTED] Solution.

Purpose: Purpose of this milestone is to verify all current capable assets are configured appropriately for [REDACTED] solution.

Evidence:

- 1) Verification from the SME within the [REDACTED] (month of September) that all assets capable of sending logs to [REDACTED] are indeed being monitored by [REDACTED] solution.
- 2) Verification from the QA team of SME verification will be documented within the [REDACTED] (month of September).

Milestone 3 - A3 Problem Solving Session

Description: Conduct an A3 problem and process solving session to identify the root cause and counter measures.

Purpose: Purpose of this milestone is to conduct an A3 process and problem solving session to do a deep dive into process(s) to identify root cause and identify countermeasures, action plan, validate impact and prevent recurrence.

Evidence:

The A3 problem solving process job aide template with completed steps 1 through 7, which derived the root cause statement and countermeasures (milestones 4 & 5).

Milestone 4 - Modify NERC CIP [REDACTED] Process

Description: Update the [REDACTED] process to include instructions for the SME to capture the verification of assets that are capable of logging, are indeed logging to [REDACTED] solution.

Purpose: Purpose of this milestone is to ensure that process prescribes on how SME should onboard and sustain assets as relates to [REDACTED] logging and monitoring.

Evidence:

Updated process document (include an approved, updated process with signatures).

Milestone 5 - Communication to SME regarding updated NERC CIP [REDACTED] Process

Description: Ensure that all SMEs have acknowledged the updated process document.

Purpose: Purpose of this milestone is to ensure that all SME's have reviewed the updated process.

Evidence:

- 1) List of current SMEs for all environments.
- 2) Announcement to all SME informing them of updated program/process using a required read.
- 3) Acknowledgement that SME has reviewed the updated program/process documents (Results of who completed the required read).

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

Proposed Completion date of Mitigation Plan: December 21, 2018

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

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Milestone 1 - Asset [REDACTED] logs are monitored by [REDACTED] server	<p>Description: Ensure that asset has correct cert file installed and the asset's logs begin being monitored by [REDACTED] server.</p> <p>Evidence: 1) The evidence will include description of how cert was updated on asset [REDACTED] on 6/25/2018. 2) The evidence will include a screenshot displaying asset [REDACTED] contains new cert. 3) The evidence will include a screenshot displaying timeline that asset [REDACTED] logs are being captured by [REDACTED]</p>	06/29/2018	06/29/2018		No
90 Days Milestone	This milestone is due to the delay while business was conducting the A3. No evidence will be provided for this milestone.	09/01/2018	09/01/2018	No evidence will be provided for this milestone.	No
Milestone 2 - SME check for extent of condition	<p>Description: In use of the [REDACTED] [REDACTED] each SMEs will conduct review of assets and attest that each asset, which can send logs is configured and being</p>	10/26/2018			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
	<p>monitored by [REDACTED] Solution.</p> <p>Evidence: 1) Verification from the SME within the [REDACTED] (month of September) that all assets capable of sending logs to [REDACTED] are indeed being monitored by [REDACTED] solution. 2) Verification from the QA team of SME verification will be documented within the [REDACTED] (month of September).</p>				
Milestone 3 - A3 Problem Solving Session	<p>Description: Conduct an A3 problem and process solving session to identify the root cause and counter measures.</p> <p>Evidence: The A3 problem solving process job aide template with completed steps 1 through 7, which derived the root cause statement and countermeasures (milestones 4 & 5).</p>	10/29/2018			No
Milestone 4 - Modify NERC CIP [REDACTED] Process	<p>Description: Update the [REDACTED] process to include instructions for the</p>	11/09/2018			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
	<p>SME to capture the verification of assets that are capable of logging, are indeed logging to [REDACTED] solution.</p> <p>Evidence: Updated process document (include an approved, updated process with signatures).</p>				
<p>Milestone 5 - Communication to SME regarding updated NERC CIP [REDACTED] Process</p>	<p>Description: Ensure that all SMEs have acknowledged the updated process document.</p> <p>Evidence: 1) List of current SMEs for all environments. 2) Announcement to all SME informing them of updated program/process using a required read. 3) Acknowledgement that SME has reviewed the updated program/process documents (Results of who completed the required read).</p>	<p>12/21/2018</p>			<p>No</p>

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.

Increased awareness and focus by SMEs when reviewing the monthly [REDACTED] report that is monitored by the [REDACTED] will minimize the risk of reoccurrence while mitigation plan is being implemented.

Prevention

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

By implementing this mitigation plan, [REDACTED] will use the updated processes to minimize the probability of this type of noncompliance happening again and therefore reduce the risk of similar violations.

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

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): RFC2018020086

Mitigated Standard Requirement(s): CIP-007-6 R4.

Scheduled Completion as per Accepted Mitigation Plan: December 21, 2018

Date Mitigation Plan completed: December 12, 2018

RF Notified of Completion on Date: December 19, 2018

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2018020086 Certification Package.zip		4,921,284

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 RFC2018020086

Standard/Requirement: CIP-007-6 R4

NERC Mitigation Plan ID: RFCMIT014196

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	Mitigation Plan Submittal	RF Acceptance	NERC Approval	Certification Submittal	Date of Completion
Self-Report 07/17/18	10/12/18	10/16/18	11/14/18	12/19/18	12/17/18

Description of Issue

[Mitigation Task RFC2018020086](#)

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	RFC2018020086 Certification Package	CIP-007-6 R4

Verification of Mitigation Plan Completion

Milestone 1: Asset [REDACTED] logs are monitored by [REDACTED] server.

Proposed Completion Date: June 29, 2018

Actual Completion Date: June 29, 2018

File 1, “RFC2018020086 Certification Package,” Milestone 1 at Pages 2 and 3, shows that the entity is now capturing logs via [REDACTED] for the referenced asset.

Milestone # 1 Completion verified.

Milestone 2: SME check for extent of condition.

Proposed Completion Date: October 26, 2018

Actual Completion Date: October 19, 2018

File 1, “*RFC2018020086 Certification Package*,” Milestone 2 at Pages 2 through 5, shows that the entity conducted an extent of condition and includes an excel workbook outlining the results.

Milestone # 2 Completion verified.

Milestone 3: A3 Problem Solving Session.

Proposed Completion Date: October 29, 2018

Actual Completion Date: October 22, 2018

File 1, “*RFC2018020086 Certification Package*,” Milestone 3 at Page 2, shows that the entity conducted an A3 problem solving session and includes a completed A3 worksheet outlining, *inter alia*, the problem, root cause, and countermeasures.

Milestone # 3 Completion verified.

Milestone 4: Modify NERC CIP [REDACTED] Process.

Proposed Completion Date: November 9, 2018

Actual Completion Date: October 30, 2018

File 1, “*RFC2018020086 Certification Package*,” Milestone 4 at Pages 2 through 81, includes the entity’s [REDACTED] process, which was revised per Milestone 4. The revision history reflects changes made on October 25, 2018 that were ultimately approved on October 30, 2018, as reflected by the dated signature line. The evidence also shows modifications to process flow diagrams, which now require the completion of compliance requirements matrices and the attachment of said matrices to applicable change orders.

Milestone # 4 Completion verified.

Milestone 5: Communication to SME regarding updated NERC CIP [REDACTED] Process.

Proposed Completion Date: December 21, 2018

Actual Completion Date: December 17, 2018

File 1, "*RFC2018020086 Certification Package*," Milestone 5 at Pages 2 through 21, shows the communications and material presented to all affected entity subject matter experts in accordance with Milestone 5.

Milestone # 5 Completion verified.

The Mitigation Plan is hereby verified complete.



Date: February 15, 2019

Anthony Jablonski
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Self Report

Entity Name: [REDACTED] ([REDACTED])

NERC ID: [REDACTED]

Standard: CIP-007-6

Requirement: CIP-007-6 R4.

Date Submitted: May 14, 2019

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED] [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: December 27, 2018

End/Expected End Date:

Reliability Functions: [REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]

Is Possible Violation still No
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: Current Practice: [REDACTED] has a [REDACTED] in place to verify NERC Cyber Assets are being logged and alerted upon per CIP007 R4 P4.1 and P4.2. The program requires that logging of security events to be enabled on each Cyber Asset per its capability. Assets with [REDACTED] or [REDACTED] operating systems are configured with an agent to send logs to the [REDACTED] [REDACTED] ([REDACTED] log aggregator These logs are then forwarded to the [REDACTED] [REDACTED] uses [REDACTED] ([REDACTED] log collection and correlation too) to perform the function of [REDACTED] along with the [REDACTED] servers. Assets which cannot send logs to [REDACTED] are configured to send logs to a [REDACTED] server and then to [REDACTED] is configured to alert upon detection of anomalies (detected successful login attempts, failed access and failed login attempts, and malicious code detection) for all assets and upon disconnects. A monthly report is generated from [REDACTED] that lists all the assets that are logging. [REDACTED] [REDACTED] is a workflow system, it has a task to track the review by subject matter experts (SME) to verify that all the assets are logging as per the requirement.

While adding asset:
A compliance matrix that requires compliance with all the applicable requirements (Including CIP007 R4, logging is enabled and is working) is used to ensure that the asset is logging (either locally or sending logs to [REDACTED] Based on the capability of the asset, if it is logging locally, manual log review procedures are enforced, if asset is sending logs to [REDACTED] log correlation

Self Report

works at the [REDACTED]

During [REDACTED] SMEs compare the assets listed in the report with the asset inventory to verify that all the assets are infect logging and the communication is working. In addition, after any change (patching included) SMEs verify that CIP005 and CIP007 controls are still effective, this includes the verification that the logging is not impacted by the change.

If the logging stops, the [REDACTED] administrators receive an alert and begin working with the asset's SME to resolve the issue.

If during review of the monthly report an anomaly and/or difference is found, the SME attempts to resolve the issue and if necessary contacts the [REDACTED] administrator for assistance.

[REDACTED] Architecture: See attachment "[REDACTED] Architecture Conceptual Diagram.pdf" for details. In summary, [REDACTED] uses agents for the assets that use [REDACTED] and [REDACTED] operating system. Out of [REDACTED] NERC assets, [REDACTED] assets logging is agent based and [REDACTED] assets are agentless. This architecture is categorized as EACMS and performs log collection and correlation for [REDACTED] assets.

[REDACTED] is responsible for reviewing a summarization or sampling of logged events for the assets that are sending logs to [REDACTED] infrastructure.

Incident Description: All the controls as designed, described in section above, were working fine as of 12/26/2018. Starting approximately at 9 am on 12/27/2018, Database engineering contacted [REDACTED] to inform that the database is performing the transactions slow. [REDACTED] application was identified as non-functional. [REDACTED] team immediately started working on it and determined that the database issue is caused by non-functional purge. A case was opened with [REDACTED] and continuous working with [REDACTED]. As the issue was not being resolved, [REDACTED] was referring to some problems with [REDACTED] configuration. [REDACTED] team started working with [REDACTED] support to resolve the problem. By the evening of 12/31/2018, application was partially recovered (application was usable for administrator interface only while events were still collected by the application), however was in a degraded state (application was not capable of collecting events). [REDACTED] work continued with [REDACTED] and [REDACTED] and the root cause of identified as a bug in [REDACTED] code, that was in the version installed initially and NOT because of any update or patching. This bug caused the database partitioning to be configured incorrectly. Based on this root cause, a restoration plan was created on 1/11/2019. The restoration plan was executed from 1/12/2019 till 1/14/2019 (See timeline for detailed restoration plan). It was expected that [REDACTED] will take a few days to process the backlog. It was noted that [REDACTED] was having issues processing the logs. Working with [REDACTED] from 1/16/2019 till 1/28/2019, this problem was solved. The applied fix was monitored and it was determined that the [REDACTED] was capturing events with some intermittent issues ([REDACTED] kept dropping the log source). While monitoring the [REDACTED] application performance seemed degraded and some agents were knocked offline. [REDACTED] event consumption stopped working again on 2/13/2019. A "critical ticket" was opened immediately with [REDACTED] and [REDACTED] started working with [REDACTED] on 2/14/2019. Working with [REDACTED] all the issues were resolved on 3/4/2019. The performance was monitored from 3/4/2019 to 3/27/2019 to conclude that the problem has been resolved.

During the monitoring from 3/4/2019 to 3/27/2019, On Tuesday March 19, [REDACTED] reached out to [REDACTED] SMEs to inform that there are 5 assets agents that are online and communicating but not sending logs ([REDACTED]). [REDACTED] went in and started doing basic troubleshooting methods, restarting the machines and stop/start services for the agent. Those steps did not resolve the

Self Report

issue. [REDACTED] and [REDACTED] SME met with [REDACTED] on Wednesday March 27th and found in the logs that the agents stopped logging due to high disk usage space. Disk space was increased on 5 assets that stopped logging and March 29th and confirmed that all the assets are checking in and sending logs.

Threshold used to monitor the disk usage is tweaked to prevent such future failures.

Additional Incident:

On Tuesday, 4/23/2019, during preparation for security patch installations for [REDACTED] it was identified that the [REDACTED] connection was down and we did not receive an alert for failed log source down. Per our process, an incident ticket [REDACTED] was created within 4 business hours and notified the stakeholders of the potential need to manually review logs. After some brief troubleshooting, it was identified that the database account that [REDACTED] uses to pull this data was not functioning correctly. [REDACTED] immediately opened a second incident ticket [REDACTED] with [REDACTED] to resolve the issue. Database engineer informed that for the configured account, the box for account expiration was not unchecked when it was created. [REDACTED] SME had the database engineer disable account expiration and then attempted to reestablish the connection and everything started working again.

Further, we investigated on when it stopped/last worked. It appears that the account expired on the 11th of April. Given that our [REDACTED] database does not store data for more than 10 days (up to 4/21/2019 from 4/11/2019), this means that we did not process two days of data (4/23 minus 4/21). The data may exist on the endpoints but we cannot process it through automated means now. It would have to be done manually, if it exists.

[REDACTED] further investigated why we did not get an alert for failed log source. It was determined that the [REDACTED] log source down alert was not configured properly to monitor the new log sources are created after we implemented the custom patches from [REDACTED] [REDACTED] reconfigured the rule to monitor the new log sources. [REDACTED] SME performed a controlled test to verify that it is now functioning.

Please see "Timeline" section for details.

While [REDACTED] and [REDACTED] infrastructure was unstable, log collection was intermittent from [REDACTED] agent based assets from 11/27/2019 till 01/10/2019 and then again from 2/13/2019 till 3/4/2019. However, the logging for agentless assets was working just fine.

This potential non-compliance was detected while [REDACTED] team was busy recovering the [REDACTED] infrastructure and a PNC was concluded on 3/27/2019.

Current protections in place?

[REDACTED] [REDACTED] is in a [REDACTED] behind a firewall. No firewall issues or self-reports were identified during the period [REDACTED] was having [REDACTED] problems.

The firewall has IDS enabled. Logging from source on the ESP would be inspected.

[REDACTED] is on the corporate network. This is one-way communication i.e. the agents on the assets collect log and send the logs to [REDACTED] Firewall does not allow communication from [REDACTED] to the assets inside the ESP.

The agented assets are compliant with all other applicable CIP requirements.

Logs collected after the partial restoration of the infrastructure on 1/10/2019 and again on 2/25/2019 shows no unauthorized activities.

Access to all the NERC assets was controlled based on need and was authorized only to NERC qualified (up-to-date training and current PRA) individuals. No Personnel (CIP004) or Physical issues/incidents (CIP006 and CIP008) or self-reports were identified during the period [REDACTED] was having

Self Report

██████ problems.

What is the problem?

After the recovery we were able to collect 43% of the missing days data during the first outage and 10% of the missing days data during the second outage because first time recovery ████████ did not process the data and we could recover from the assets (██████). However, for second recovery the ████████ had already processed the data and began to purge it, hence only 10% of data, for 100% of the assets, causing violation of CIP007 R4 Part 4.1.

During the outage, the alerts for security events could not be generated for ████████ assets, causing violation of CIP007 R4 Part 4.2

The review of summarization of logs for ████████ agented assets was not performed during the outage, causing violation of CIP007-6 R4, Part 4.4. Correlation rules ran after restored generated alerts that were investigated and no malicious activity was noted. Mostly account hygiene issues were identified.

Root Cause of Possible Violation: A contributing factor was a bug in the software caused the database partitioning to be configured incorrectly. However, the root cause is determined to be a lack of escalation in the current ████████ process. While ████████ team was busy recovering the infrastructure, the escalation should have informed the asset owners of the infrastructure issues so that the local review of summarization of logs could be performed. How was the violation discovered? ████████ team informed ████████ of the violation that we may have lost the logs. However, after the restoration, it was determined on 3/27/2018 that the summarization of logs was not reviewed every 15 days (three cycles) from 12/27/2018 till 3/4/2019.

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

The Non-compliance is determined to be related to lack of escalation in current ████████ process.

Timeline:

12/27/2018

- @9am ████████ Application identified as non-functional
- @10am ████████ team determined database issue caused by non-functional purge
- @10:30am Critical Case # ████████ opened with ████████
- @10:40am ████████ response. Troubleshooting ████████ initiated.
- @1pm It was determined that the purge command was working but working abnormally slowly.
- @1pm In order to recover application functionality to continue troubleshooting a manual purge of the oldest events from the database would need to be completed. Based on purge performance this process was expected to take several days. Manual purge started
- @1pm ████████ believed the problem to be caused by the ████████ select statement not containing a no lock statement. Disabled ████████ interface. Ticket opened with ████████

12/28-12/30/2018

- Manual purge continued

12/31/2018

- Manual Purge completed.
- Application partially recovered. Remained in a degraded state but we were able to continue troubleshooting with ████████

1/1/2019-1/10/2019

- Continued to work with ████████ and ████████

1/11/2019

- ████████ ruled out as cause of purge issue
- ████████ escalated to ████████
- Root cause identified. Bug in ████████ ████████ code caused the database

Self Report

partitioning to be configured incorrectly.

- Restoration plan documented
- Began execution of restoration plan

Restoration Plan was created on 1/11/2019 with the following steps

1. Disable both [REDACTED] application servers (Complete)
2. Initiate a Full Recovery Backup (In progress)
3. Connect [REDACTED] to the [REDACTED] Database and allow it to collect all remaining events (In progress)
4. Check all application account permissions on the [REDACTED] instance
5. Truncate Events table
6. Perform a second Full Recovery Backup after truncation completes
7. Perform the upgrade to [REDACTED] on the primary management server
8. Verify purge settings and functionality
9. Perform the upgrade to [REDACTED] on the secondary management server
10. Verify functionality
11. Verify connection to agents re-established
12. Restore [REDACTED] connectivity.

1/12-1/14/2019

- Continued execution of recovery plan
- Performed upgrade to [REDACTED] to reconfigure the partitioning correctly
- Application recovered

1/15/2019

- [REDACTED] connectivity reestablished
- [REDACTED] [REDACTED] needs to process backlogged events
- [REDACTED] consumption expected to take several days

1/16/2019-1/18

- Issue with [REDACTED] event consumption. [REDACTED] was not processing events older than the day [REDACTED] connectivity was reestablished.
- Case opened with [REDACTED] and resolution provided

1/21/2019

- [REDACTED] provided resolution was not working correctly

1/24/2019

- Submitted request to Database team to have first 25 million events inserted into new table to recovery data

1/26/2019

- Database team completed work. Event INSERT is complete. [REDACTED] starts import of these events.

1/28/2019

- [REDACTED] finishes importing 25 million events.

1/28-2/12/2019

- [REDACTED] was capturing events with some intermittent issues
- While monitoring the [REDACTED] application performance seemed degraded and some agents were knocked offline while [REDACTED] query running.
- Had more processors added to the database server per database team suggestions.
- This did not resolve the database performance issues but did increase performance

2/13/2019

- [REDACTED] event consumption stopped working.
- Attempted to troubleshoot the log source but it would not reconnect
- All signs pointed to lack of ([REDACTED] statement in [REDACTED] database query as the cause of issues

2/14/2019

- @9:39 AM A second critical [REDACTED] Support ticket was submitted requesting a

Self Report

() statement be added to the query.

- @10:31 AM Responded. They suggested that this can't be resolved through support and a request for enhancement would have to be submitted.
- opened
- @ 2:12 PM requested logs
- requested issue be raised through level 3 support not the RFE process.

2/15/2019

- @8:31 AM escalated to level 3 support engineers
- @10:00 AM scheduled with level 2 support. No level 3 support provided. Level 2 support upgraded the protocol but did not add () to the statement
- @3:58 PM No resolution. Still no connectivity.
- Logs requested by and we were assured it would be escalated to level 3 support

2/16-2/18/2019

- No response from level 3 engineers

2/19/2019

- requested we run () on the database and provide time to completion

2/20/2019

- sent response ensure that level 3 engineers were involved and asked if we could help them test a custom file. We agreed to help.

2/21/2019

- Level 3 engaged
- Setup to install and test custom file #1
- Custom file #1 installed
- database disk filled due to database shrink not occurring. Had to open a support case with () to resolve. Band-aid fix brought the issue under control quickly so we could continue to work with ()
- The custom #1 did not work. () was still not added to the Query as requested
- Custom file #2 installed.
- The custom #2 did not work. () was still not added to the Query as requested

2/22/2019

- Custom file #3 installed. () was added to the Query as requested
- The custom #3 did not work. Properties file was not updating at all. Should update after every query. Appeared to be a timeout issue.
- provided some troubleshooting steps to perform then we uploaded the logs
- Custom file #4 installed.
- The custom #4 did not work. Properties file was still not updating at all.
- Asked () to work with me through the weekend. () informed me that they do not work weekends
- Due to () purge settings needing to be set @ 10 days, data began to purge before connectivity to () was established.

2/25/2019

- Custom file #5 installed.
- The custom #5 did not work. Properties file was still not updating at all.
- Custom file #6 installed.
- The custom #6 did not work. Properties file was still not updating at all.
- said that the file would not work until we optimized the database by re-indexing. This was not an option.
- We began to troubleshoot without () We noticed that a 3rd party tool (non- () Non- () that used the same internal () driver as () was having the same issue. We determined a database restart was necessary. We also determined that the prepared statements option in () has to be

Self Report

disabled. All connectivity began to work and was looking really good.

2/26-2/27/2019

- Custom #5 contained debug statements which filled up logs on
- Custom #6 provided and installed.

2/28/2019

- connectivity stopped. We determined that it was likely due to the EPS throttling due to license restrictions and worked to obtain a new license
- connectivity reestablished after EPS throttling increased

3/1/2019

- License obtained and imported
- continued to work through the weekend

3/4/2019

- issue determined to be resolved.
- Worked with to make custom #6 permanent. Testing and roll-out went smooth.

3/5/2019

- Case with closed.

3/4-3/27/2019

- Monitored the performance of infrastructure for approximately a month to conclude that it is stable.

Mitigating Activities:

Description of Mitigating Activities and Preventative

Measure: infrastructure recovery is completed and is performing its intended function.

Mitigating and Preventative Activities:

will explore to include test of alerts in current process.

Review and update (if required) the CIP009 recovery procedure to ensure that the recovery procedure is usable in the scenario where infrastructure is down.

A checklist including standard functional configuration will be created to ensure that when infrastructure is recovered we will have a functional configuration.

Update System Monitoring Process with an escalation, to initiate manual log reviews and more timely data preservation.

Require read of the updated process.

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe

Actual Impact to BPS: Minimal

Description of Potential and Potential Impact:

Actual Impact to BPS: Potential impact is determined to be high, because failing to monitor assets and generate alerts for security events creates a significant gap that a

Self Report

wrongdoer could exploit and leverage to attack the entity and BES. Such an attack likely would have been undetected.

Actual Impact:

Actual impact is determined to be lower because logs correlation and review after the restore shows no unauthorized activities. Correlation of logs is automated through [REDACTED] as noted in [REDACTED] program.

Risk Assessment of Impact to BPS: Given that it is a failure of infrastructure, but we have opportunity to improve [REDACTED] process, overall risk is determined to be lower. Potential impact is determined to be high, because failing to monitor assets and generate alerts for security events creates a significant gap that a wrongdoer could exploit and leverage to attack the entity and BES. Such an attack likely would have been undetected. However, actual impact is determined to be lower because logs correlation and review after the restore shows no unauthorized activities.

Additional Entity Comments: All the assets were accounted for after the recovery. [REDACTED] assets were identified to be reporting out of [REDACTED]. Remaining [REDACTED] assets were corrected immediately.

Partial system recovery on 12/27/2018 but a plan to restore not created until 1/11/2019 (11 days after partial recovery already occurred) because we were in the troubleshooting mode and did not know if the problem was due to [REDACTED] ([REDACTED] or [REDACTED] [REDACTED])

[REDACTED] will be meeting with [REDACTED] management to review and determine if [REDACTED] infrastructure is scaled to handle to load.

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
RFC2019021564	CIP-007-6 R4.	

Mitigation Plan Submitted On: May 24, 2019

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: July 15, 2019

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] [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		
RFC2019021564	12/27/2018	CIP-007-6 R4.

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 R4 – Security Event Monitoring.

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

Current Practice: [REDACTED] has a [REDACTED] in place to verify NERC Cyber Assets are being logged and alerted upon per CIP007 R4 P4.1 and P4.2. The program requires that logging of security events to be enabled on each Cyber Asset per its capability. Assets with [REDACTED] or [REDACTED] operating systems are configured with an agent to send logs to the [REDACTED] ([REDACTED] log aggregator. These logs are then forwarded to the [REDACTED] ([REDACTED] uses [REDACTED] ([REDACTED] log collection and correlation too) to perform the function of [REDACTED] along with the [REDACTED] servers. Assets which cannot send logs to [REDACTED] are configured to send logs to a [REDACTED] server and then to [REDACTED] is configured to alert upon detection of anomalies (detected successful login attempts, failed access and failed login attempts, and malicious code detection) for all assets and upon disconnects. A monthly report is generated from [REDACTED] that lists all the assets that are logging. [REDACTED] [REDACTED] is a workflow system, it has a task to track the review by subject matter experts (SME) to verify that all the assets are logging as per the requirement.

While adding asset:

A compliance matrix that requires compliance with all the applicable requirements (Including CIP007 R4, logging is enabled and is working) is used to ensure that the asset is logging (either locally or sending logs to [REDACTED] Based on the capability of the asset, if it is logging locally, manual log review procedures are enforced, if asset is sending logs to [REDACTED] log correlation works at the [REDACTED]

During [REDACTED]

SMEs compare the assets listed in the report with the asset inventory to verify that all the assets are infect logging and the communication is working. In addition, after any change (patching included) SMEs verify that CIP005 and CIP007 controls are still effective, this includes the verification that the logging is not impacted by the change.

If the logging stops, the [REDACTED] ([REDACTED] [REDACTED] administrators receive an alert and begin working with the asset's SME to resolve the issue.

If during review of the monthly report an anomaly and/or difference is found, the SME attempts to resolve the issue and if necessary contacts the [REDACTED] [REDACTED] administrator for assistance.

[REDACTED] Architecture: See attachment "[REDACTED] Architecture Conceptual Diagram.pdf" for details. In summary, [REDACTED] uses agents for the assets that use [REDACTED] and [REDACTED] operating system. Out of [REDACTED] [REDACTED] NERC assets, [REDACTED] assets logging is agent based and [REDACTED] assets are agentless. This architecture is categorized as EACMS and performs log collection and correlation for [REDACTED] assets. [REDACTED] is responsible for reviewing a summarization or sampling of logged events for the assets that are sending logs to [REDACTED] infrastructure.

Incident Description: All the controls as designed, described in section above, were working fine as of 12/26/2018. Starting approximately at 9 am on 12/27/2018, [REDACTED] contacted [REDACTED] to inform that the database is performing the transactions slow. [REDACTED] [REDACTED] ([REDACTED] application was identified as non-functional. [REDACTED] team immediately started working on it and determined that the database issue is caused by non-functional purge. A case was opened with [REDACTED] and continuous working with [REDACTED] As the issue was not being resolved, [REDACTED] was referring to some problems with [REDACTED] [REDACTED] configuration. [REDACTED] team started working with [REDACTED] support to resolve

the problem. By the evening of 12/31/2018, application was partially recovered (application was usable for administrator interface only while events were still collected by the application), however was in a degraded state (application was not capable of collecting events). [REDACTED] work continued with [REDACTED] and [REDACTED] and the root cause of identified as a bug in [REDACTED] [REDACTED] code, that was in the version installed initially and NOT because of any update or patching. This bug caused the database partitioning to be configured incorrectly. Based on this root cause, a restoration plan was created on 1/11/2019. The restoration plan was executed from 1/12/2019 till 1/14/2019 (See timeline for detailed restoration plan). It was expected that [REDACTED] will take a few days to process the backlog. It was noted that [REDACTED] was having issues processing the logs. Working with [REDACTED] from 1/16/2019 till 1/28/2019, this problem was solved. The applied fix was monitored and it was determined that the [REDACTED] was capturing events with some intermittent issues ([REDACTED] kept dropping the log source). While monitoring the [REDACTED] application performance seemed degraded and some agents were knocked offline. [REDACTED] event consumption stopped working again on 2/13/2019. A "critical ticket" was opened immediately with [REDACTED] and [REDACTED] started working with [REDACTED] on 2/14/2019. Working with [REDACTED] all the issues were resolved on 3/4/2019. The performance was monitored from 3/4/2019 to 3/27/2019 to conclude that the problem has been resolved.

During the monitoring from 3/4/2019 to 3/27/2019, On Tuesday March 19, [REDACTED] reached out to [REDACTED] SMEs to inform that there are 5 assets agents that are online and communicating but not sending logs ([REDACTED]). [REDACTED] team ([REDACTED] went in and started doing basic troubleshooting methods, restarting the machines and stop/start services for the agent. Those steps did not resolve the issue. [REDACTED] and [REDACTED] SME met with [REDACTED] on Wednesday March 27th and found in the logs that the agents stopped logging due to high disk usage space. Disk space was increased on 5 assets that stopped logging and March 29th and confirmed that all the assets are checking in and sending logs.

Threshold used to monitor the disk usage is tweaked to prevent such future failures.

Additional Incident:

On Tuesday, 4/23/2019, during preparation for security patch installations for [REDACTED] it was identified that the [REDACTED] [REDACTED] connection was down and we did not receive an alert for failed log source down. Per our process, an incident ticket [REDACTED] was created within 4 business hours and notified the stakeholders of the potential need to manually review logs. After some brief troubleshooting, it was identified that the database account that [REDACTED] uses to pull this data was not functioning correctly. [REDACTED] immediately opened a second incident ticket [REDACTED] with [REDACTED] to resolve the issue. Database engineer informed that for the configured account, the box for account expiration was not unchecked when it was created. [REDACTED] SME had the database engineer disable account expiration and then attempted to reestablish the connection and everything started working again.

Further, we investigated on when it stopped/last worked. It appears that the account expired on the 11th of April. Given that our [REDACTED] database does not store data for more than 10 days (up to 4/21/2019 from 4/11/2019), this means that we did not process two days of data (4/23 minus 4/21). The data may exist on the endpoints but we cannot process it through automated means now. It would have to be done manually, if it exists.

[REDACTED] further investigated why we did not get an alert for failed log source. It was determined that the [REDACTED] log source down alert was not configured properly to monitor the new log sources are created after we implemented the custom patches from [REDACTED] [REDACTED] reconfigured the rule to monitor the new log sources. [REDACTED] SME performed a controlled test to verify that it is now functioning.

Please see "Timeline" section for details.

While [REDACTED] and [REDACTED] infrastructure was unstable, log collection was intermittent from [REDACTED] agent based assets from 11/27/2019 till 01/10/2019 and then again from 2/13/2019 till 3/4/2019. However, the logging for agentless assets was working just fine.

This potential non-compliance was detected while [REDACTED] team was busy recovering the [REDACTED] infrastructure and a PNC was concluded on 3/27/2019.

Current protections in place?

[REDACTED] [REDACTED] is in a [REDACTED] behind a firewall. No firewall issues or self-reports were identified during the

period [REDACTED] was having [REDACTED] problems.

The firewall has IDS enabled. Logging from source on the ESP would be inspected.

[REDACTED] is on the corporate network. This is one-way communication i.e. the agents on the assets collect log and send the logs to [REDACTED]. Firewall does not allow communication from [REDACTED] to the assets inside the ESP.

The agented assets are compliant with all other applicable CIP requirements.

Logs collected after the partial restoration of the infrastructure on 1/10/2019 and again on 2/25/2019 shows no unauthorized activities.

Access to all the NERC assets was controlled based on need and was authorized only to NERC qualified (up-to-date training and current PRA) individuals. No Personnel (CIP004) or Physical issues/incidents (CIP006 and CIP008) or self-reports were identified during the period [REDACTED] was having [REDACTED] problems.

What is the problem?

After the recovery we were able to collect 43% of the missing days data during the first outage and 10% of the missing days data during the second outage because first time recovery [REDACTED] did not process the data and we could recover from the assets ([REDACTED]). However, for second recovery the [REDACTED] had already processed the data and began to purge it, hence only 10% of data, for 100% of the assets, causing violation of CIP007 R4 Part 4.1.

During the outage, the alerts for security events could not be generated for [REDACTED] assets, causing violation of CIP007 R4 Part 4.2

The review of summarization of logs for [REDACTED] agented assets was not performed during the outage, causing violation of CIP007-6 R4, Part 4.4. Correlation rules ran after restored generated alerts that were investigated and no malicious activity was noted. Mostly account hygiene issues were identified.

Root Cause of Possible Violation: A contributing factor was a bug in the software caused the database partitioning to be configured incorrectly. However, the root cause is determined to be a lack of escalation in the current [REDACTED] process. While [REDACTED] team was busy recovering the infrastructure, the escalation should have informed the asset owners of the infrastructure issues so that the local review of summarization of logs could be performed.

Explain how is it determined that the Noncompliance is related to documentation, performance, or both.
The Non-compliance is determined to be related to lack of escalation in current [REDACTED] process.

Timeline:

- 12/27/2018 • @9am [REDACTED] Application identified as non-functional
- @10am [REDACTED] team determined database issue caused by non-functional purge
- @10:30am Critical Case # [REDACTED] opened with [REDACTED]
- @10:40am [REDACTED] response. Troubleshooting [REDACTED] initiated.
- @1pm It was determined that the purge command was working but working abnormally slowly.
- @1pm In order to recover application functionality to continue troubleshooting a manual purge of the oldest events from the database would need to be completed. Based on purge performance this process was expected to take several days. Manual purge started
- @1pm [REDACTED] believed the problem to be caused by the [REDACTED] select statement not containing a no lock statement. Disabled [REDACTED] interface. Ticket opened with [REDACTED]
- 12/28-12/30/2018 • Manual purge continued
- 12/31/2018 • Manual Purge completed.
- Application partially recovered. Remained in a degraded state but we were able to continue troubleshooting with [REDACTED]
- 1/1/2019-1/10/2019 • Continued to work with [REDACTED] and [REDACTED]
- 1/11/2019 • [REDACTED] ruled out as cause of purge issue
- [REDACTED] escalated to [REDACTED]
- Root cause identified. Bug in [REDACTED] code caused the database partitioning to be configured incorrectly.
- Restoration plan documented

- Began execution of restoration plan

Restoration Plan was created on 1/11/2019 with the following steps

1. Disable both [REDACTED] application servers (Complete)
2. Initiate a Full Recovery Backup (In progress)
3. Connect [REDACTED] to the [REDACTED] Database and allow it to collect all remaining events (In progress)
4. Check all application account permissions on the [REDACTED] instance
5. Truncate Events table
6. Perform a second Full Recovery Backup after truncation completes
7. Perform the upgrade to [REDACTED] on the primary management server
8. Verify purge settings and functionality
9. Perform the upgrade to [REDACTED] on the secondary management server
10. Verify functionality
11. Verify connection to agents re-established
12. Restore [REDACTED] connectivity.

1/12-1/14/2019 • Continued execution of recovery plan

- Performed upgrade to [REDACTED] to reconfigure the partitioning correctly
- Application recovered

1/15/2019 • [REDACTED] connectivity reestablished

- [REDACTED] needs to process backlogged events
- [REDACTED] consumption expected to take several days

1/16/2019-1/18 • Issue with [REDACTED] event consumption. [REDACTED] was not processing events older than the day [REDACTED] connectivity was reestablished.

- Case opened with [REDACTED] and resolution provided

1/21/2019 • [REDACTED] provided resolution was not working correctly

1/24/2019 • Submitted request to Database team to have first 25 million events inserted into new table to recovery data

1/26/2019 • Database team completed work. Event INSERT is complete. [REDACTED] starts import of these events.

1/28/2019 • [REDACTED] finishes importing 25 million events.

1/28-2/12/2019 • [REDACTED] was capturing events with some intermittent issues

- While monitoring the [REDACTED] application performance seemed degraded and some agents were knocked offline while [REDACTED] query running.

- Had more processors added to the database server per database team suggestions.

- This did not resolve the database performance issues but did increase performance

2/13/2019 • [REDACTED] event consumption stopped working.

- Attempted to troubleshoot the log source but it would not reconnect

- All signs pointed to lack of ([REDACTED] statement in [REDACTED] database query as the cause of issues

2/14/2019 • @9:39 AM A second critical [REDACTED] Support ticket was submitted requesting a ([REDACTED]) statement be added to the query.

- @10:31 AM [REDACTED] Responded. They suggested that this can't be resolved through support and a request for enhancement would have to be submitted.

- [REDACTED] 129997 opened

@ 2:12 PM [REDACTED] requested logs

- [REDACTED] requested issue be raised through level 3 support not the [REDACTED] process.

2/15/2019 • @8:31 AM [REDACTED] escalated to level 3 support engineers

- @10:00 AM [REDACTED] scheduled with level 2 support. No level 3 support provided. Level 2 support upgraded the [REDACTED] protocol but did not add ([REDACTED]) to the statement

- @3:58 PM No resolution. Still no connectivity.

- Logs requested by [REDACTED] and we were assured it would be escalated to level 3 support

2/16-2/18/2019 • No response from [REDACTED] level 3 engineers

2/19/2019 • [REDACTED] requested we run [REDACTED] on the database and provide time to completion

2/20/2019 • [REDACTED] sent response ensure that level 3 engineers were involved and asked if we could help them test a custom [REDACTED] file. We agreed to help.

2/21/2019 • Level 3 engaged

- WebEx Setup to install and test custom [REDACTED] file #1

- Custom [REDACTED] file #1 installed

- [REDACTED] database disk filled due to database shrink not occurring. Had to open a support case with [REDACTED] to resolve. Band-aid fix brought the issue under control quickly so we could continue to work

with [REDACTED]

- The custom [REDACTED] #1 did not work. ([REDACTED] was still not added to the [REDACTED] Query as requested
- Custom [REDACTED] file #2 installed.
- The custom [REDACTED] #2 did not work. ([REDACTED] was still not added to the [REDACTED] Query as requested
- 2/22/2019 • Custom [REDACTED] file #3 installed. ([REDACTED] was added to the [REDACTED] Query as requested
- The custom [REDACTED] #3 did not work. Properties file was not updating at all. Should update after every query. Appeared to be a timeout issue.
- [REDACTED] provided some troubleshooting steps to perform then we uploaded the logs
- Custom [REDACTED] file #4 installed.
- The custom [REDACTED] #4 did not work. Properties file was still not updating at all.
- Asked [REDACTED] to work with me through the weekend. [REDACTED] informed me that they do not work weekends
- Due to [REDACTED] [REDACTED] purge settings needing to be set @ 10 days, data began to purge before connectivity to [REDACTED] was established.
- 2/25/2019 • Custom [REDACTED] file #5 installed.
- The custom [REDACTED] #5 did not work. Properties file was still not updating at all.
- Custom [REDACTED] file #6 installed.
- The custom [REDACTED] #6 did not work. Properties file was still not updating at all.
- [REDACTED] said that the file would not work until we optimized the database by re-indexing. This was not an option.
- We began to troubleshoot without [REDACTED] We noticed that a 3rd party tool (non-[REDACTED] Non-[REDACTED] that used the same internal [REDACTED] driver as [REDACTED] was having the same issue. We determined a database restart was necessary. We also determined that the prepared statements option in [REDACTED] has to be disabled. All connectivity began to work and was looking really good.
- 2/26-2/27/2019 • Custom [REDACTED] #5 contained debug statements which filled up logs on [REDACTED]
- Custom [REDACTED] #6 provided and installed.
- 2/28/2019 • [REDACTED] connectivity stopped. We determined that it was likely due to the EPS throttling due to license restrictions and worked to obtain a new license
- [REDACTED] connectivity reestablished after EPS throttling increased
- 3/1/2019 • License obtained and imported
- [REDACTED] continued to work through the weekend
- 3/4/2019 • [REDACTED] issue determined to be resolved.
- Worked with [REDACTED] to make custom [REDACTED] #6 permanent. Testing and roll-out went smooth.
- 3/5/2019 • Case with [REDACTED] closed.
- 3/4-3/27/2019 • Monitored the performance of infrastructure for approximately a month to conclude that it is stable.

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

[REDACTED] team informed [REDACTED] of the violation that we may have lost the logs. However, after the restoration, it was determined on 3/27/2018 that the summarization of logs was not reviewed every 15 days (three cycles) from 12/27/2018 till 3/4/2019.

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: Update "System Monitoring Process"

Description: This milestone directly countermeasures the root cause.

The update will include:

- a) Escalation to initiate manual log reviews and more timely data preservation.
- b) Test of alerts
- c) Enhanced monitoring of logging infrastructure

Purpose: The updates will help prevent the violations by informing the SMEs of the logging failures, if the logging infrastructure is down in future. In addition, a regular testing of alerts will ensure that the logging infrastructure as configured is working. [REDACTED] is adding an enhanced monitoring of logging infrastructure as well.

Evidence: Updated "System Monitoring Process" with revision history.

Milestone 2: Perform a required read of updated "System Monitoring Process"

Description: This milestone directly countermeasures the root cause. The updated process will be communicated to the impacted users of the process using the required read.

Purpose: Ensure that the updated system monitoring process is communicated to all the impacted SMEs and that they acknowledge the updates.

Evidence: An output from [REDACTED] learning management system showing the population and the completion history of the required read.

Milestone 3: Create a checklist including standard functional configuration

Description: It was noted during recovery of the [REDACTED] infrastructure that we had another outage because we did not set one configuration that resulted in loss of data for 2 days.

Purpose: To ensure that when infrastructure is recovered we will have a functional configuration.

Evidence: A newly created checklist with standard functional configuration.

Milestone 4: Review and update the CIP009 recovery procedure to include data recovery

Description: It was noted during recovery of the [REDACTED] infrastructure that the current CIP009 recovery procedure does not list how to recover data. Making the CIP009 recovery procedure useable will ensure quicker recovery in future.

Purpose: To ensure that the recovery procedure is usable for data recovery in future failures.

Evidence: An updated CIP009 recovery procedure with revision history.

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 15, 2019

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: Update "System Monitoring Process"	This milestone directly countermeasures the root cause. The update will include: a) Escalation to initiate manual log reviews and more timely data preservation. b) Test of alerts c) Enhanced Start monitoring of logging infrastructure	06/20/2019			No
Milestone 2: Review and update the CIP009 recovery procedure	It was noted during recovery of the [REDACTED] infrastructure that the current CIP009 recovery procedure does not list how to recover data. Making the CIP009 recovery procedure useable will ensure quicker recovery in future.	06/28/2019			No
Milestone 3: Create a checklist including standard functional configuration	Description: It was noted during recovery of the [REDACTED] infrastructure that we had another outage because we did not set one configuration that resulted in loss of data for 2 days. To ensure that when infrastructure is recovered we will have a functional configuration.	06/28/2019			No
Milestone 4: Perform a required read of	This milestone directly	07/15/2019			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
updated "System Monitoring Process	countermeasures the root cause. The updated process will be communicated to the impacted users of the process using the required read.				

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.

Logging infrastructure is managed centrally by [REDACTED] While the mitigation plan is being implemented, [REDACTED] team is closely watching the health and also the logging from assets.

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 plan includes updating the system monitoring process to include escalation, test of alerts, and enhanced monitoring. The updated process will be required read to all the SMEs. In addition, a standard configuration checklist will help us ensure correct configuration in future failures.

In addition, existing controls as documented below help us ensure that the logging is enabled and working:
While adding asset:

A compliance matrix that requires compliance with all the applicable requirements (Including CIP007 R4, logging is enabled and is working) is used to ensure that the asset is logging (either locally or sending logs to [REDACTED] Based on the capability of the asset, if it is logging locally, manual log review procedures are enforced, if asset is sending logs to [REDACTED] log correlation works at the [REDACTED]

During [REDACTED] SMEs compare the assets listed in the report with the asset inventory to verify that all the assets are infect logging and the communication is working. In addition, after any change (patching included) SMEs verify that CIP005 and CIP007 controls are still effective, this includes the verification that the logging is not impacted by the change.

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

All the assets were accounted for after the recovery. [REDACTED] assets were identified to be reporting out of [REDACTED] Remaining [REDACTED] assets were corrected immediately.

Partial system recovery was on 12/27/2018 but a plan to restore not created until 1/11/2019 (11 days after partial recovery already occurred) because we were in the troubleshooting mode and did not know if the problem was due to [REDACTED] ([REDACTED] or [REDACTED] ([REDACTED])

[REDACTED] will be meeting with [REDACTED] ([REDACTED] management to review and determine if [REDACTED] infrastructure is scaled to handle to load.

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): RFC2019021564

Mitigated Standard Requirement(s): CIP-007-6 R4.

Scheduled Completion as per Accepted Mitigation Plan: August 15, 2019

Date Mitigation Plan completed: August 12, 2019

RF Notified of Completion on Date: August 15, 2019

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[REDACTED] Architecture Conceptual Diagram.pdf		123,178
Entity	RFC2019021564 Certification Package.zip		4,502,108

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 RFC2019021564

Standard/Requirement: CIP-007-6 R4

NERC Mitigation Plan ID: RFCMIT014560

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	Mitigation Plan Submittal	RF Acceptance	NERC Approval	Certification Submittal	Date of Completion
Self-Report 05/14/19	05/24/19	05/28/19	06/21/19	08/15/19	08/03/19

Description of Issue

[MITIGATION PLAN RFC2019021564](#)

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	Architecture Conceptual Diagram	CIP-007-6 R4
File 2	Milestone 1	CIP-007-6 R4
File 3	Milestone 2	CIP-007-6 R4
File 4	Milestone 3	CIP-007-6 R4
File 5	Milestone 4	CIP-007-6 R4
File 6	RFC2019021564 Certification Package Cover Page	CIP-007-6 R4

Verification of Mitigation Plan Completion

Milestone 1: Milestone 1: Update “System Monitoring Process.”

Proposed Completion Date: June 20, 2019

Actual Completion Date: May 24, 2019 (reflected on Page 5 Email)

“File 2 Milestone 1,” at Pages 2 through 3, contains screenshots evidencing that the [REDACTED] has been updated to reference the newly created process documented in the [REDACTED] Monitoring Failure Process. Pages 4 through 5 show the script that was developed to test alerting functionality, the output of the script, and the enhancements made to the logging infrastructure via [REDACTED] Health. Page 22 reflects the changes made to the Entity [REDACTED] on April 29, 2019, and Page 24 shows the procedure being accepted and signed on April 30, 2019.

Milestone #1 Completion verified.

Milestone 2: Milestone 2: Review an update the CIP009 recover procedure.

Proposed Completion Date: June 28, 2019

Actual Completion Date: June 20, 2019 (reflected on Page 39 signature page)

“File 3 Milestone 2,” at Pages 2 through 39, shows the update to the recovery procedure. Page 14 shows the new section added “5.3 [REDACTED] Bulk Load Data Recovery Procedure.” The revision is also reflected via the change revision table on Page 37, stating the revision was completed on June 20, 2019. Page 39 shows that the procedure was signed and accepted by the IT Manager on June 20, 2019.

Milestone #2 Completion verified.

Milestone 3: Milestone 3: Create a checklist including standard functional configuration.

Proposed Completion Date: June 28, 2019

Actual Completion Date: June 20, 2019 (reflected on Page 6)

“File 4 Milestone 3,” at Pages 2 through 6, show the checklist that was created and used to ensure proper communication channels are established between the [REDACTED] and the log aggregation system and to ensure log aggregation system failure alerts are functional within the [REDACTED]. Page 6 shows the document was created on June 20, 2019.

Milestone #3 Completion verified.

Milestone 4: Milestone 4: Perform a required read of updated “System Monitoring Process.”

Proposed Completion Date: July 15, 2019

Actual Completion Date: August 3, 2019 (Reflected on Page 18 when last user completed task)

“File 5 Milestone 4,” at Pages 1 through 18, shows that that the entity pushed a “required read” training to affected personnel because of the updates to its process. Pages 12 through 18 show the list of SMEs who were targeted for this required read and corresponding completion dates. During this exercise, 4 personnel had their CIP access removed thus reducing the number from [REDACTED].

Milestone #4 Completion verified.

The Mitigation Plan is hereby verified complete.



Date: October 2, 2019

Anthony Jablonski
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Attachment 11

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

- 11.a The Entity's Self-Report (RFC2017016888);
- 11.b The Entity's Mitigation Plan designated as RFCMIT012746 submitted [REDACTED];
- 11.c The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
- 11.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED]

Self Report

Entity Name: [REDACTED] ([REDACTED])

NERC ID: [REDACTED]

Standard: CIP-007-6

Requirement: CIP-007-6 R5.

Date Submitted: January 23, 2017

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED] [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: July 01, 2016

End/Expected End Date:

Region Initially Determined a
Violation On:

Reliability Functions: [REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]

Is Possible Violation still No
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: On 03/01/2016, an internal Annual Vulnerability Assessment conducted at [REDACTED] identified four shared accounts on [REDACTED] assets that did not meet CIP-007-6 Part 5.5.2 "Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset." Shared account password lengths for the [REDACTED] assets were [REDACTED]
[REDACTED]
[REDACTED] A total of [REDACTED] users have access to the four shared accounts on [REDACTED]. All of these [REDACTED] people have required NERC training; background check performed, and has a need to know.

Per the local [REDACTED] vulnerability management process, internal vulnerability assessments are provided to the corporate [REDACTED] [REDACTED] group for review and determination of vulnerabilities to [REDACTED] assets/systems. If a vulnerability exists, a ticket is opened (through the [REDACTED] Hotline) and a Remediation Team is used to evaluate the impact on any [REDACTED] assets. If the Remediation Team impact analysis indicates no threat to the [REDACTED] [REDACTED] environment, the

Self Report

ticket is updated and closed. If the Remediation Team impact analysis determines the vulnerability impact is "Critical" to [REDACTED] operations, a Remediation ticket will be opened and the Remediate Vulnerability Process will begin. On affected [REDACTED] assets, the responsible Cyber Subject Matter Expert(s) (SMEs) will assume ownership of the identified vulnerability and mitigation.

The internal vulnerability assessment was handed off by the [REDACTED] SME to the [REDACTED] group in the second quarter of 2016. A vulnerability review was completed by [REDACTED] on 07/29/2016 however; there was no evidence of a ticket being opened for an impact evaluation nor was there evidence of a ticket being opened to initiate the Remediate Vulnerability process. The [REDACTED] [REDACTED] verified with the [REDACTED] SME on 12/19/2016 that no mitigation plan was generated for any of the issues identified in the 03/01/2016 [REDACTED] Annual Vulnerability Assessment.

*Cause of Possible Violation: The local [REDACTED] vulnerability management process was not followed as designed and there was no escalation built into the process when it was not carried out or not carried out properly.

*How was the violation discovered? The [REDACTED] group discovered the violation during their monthly internal audit of [REDACTED] BCAs. [REDACTED] November 2016 audit randomly sampled [REDACTED] assets, discovered the shared account violation late in the month, and reported the issue to the [REDACTED] on 12/01/2016.

*Timeline:
03/01/2016: [REDACTED] Annual Vulnerability Assessment discovery of [REDACTED] asset shared accounts that violated CIP-007-6 Part 5.5 standards for password complexity requirements.
2nd Quarter 2016: Annual Vulnerability Assessment handed off from [REDACTED] to [REDACTED] to conduct a review and impact analysis.
07/29/2016 Vulnerability review was completed by [REDACTED]
12/01/2016 Discovery of [REDACTED] asset shared accounts violation during routine [REDACTED] conducted by [REDACTED] group.
12/03/2016: [REDACTED] brought the [REDACTED] assets into compliance by using [REDACTED]
[REDACTED]
[REDACTED]

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Mitigating Activities: On 12/03/2016, [REDACTED] brought the [REDACTED] assets into compliance by using [REDACTED]
[REDACTED]
[REDACTED]

Preventive Measure: Preventive measures called out in the local [REDACTED] vulnerability management process were not followed resulting in non-compliance.

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 high due to the documented process for password-only authentication for interactive shared account access did not procedurally enforce minimum password complexity requirements.

Self Report

The actual impact to the BPS is low due to only personnel with the requisite NERC Critical Infrastructure Security Training and NERC CIP Personnel Risk Assessment (background check from HR) have access to shared accounts for the [REDACTED] assets.

Risk Assessment of Impact to [REDACTED] identifies that that potential impact to the BPS is low.
BPS: [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: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2017016888	CIP-007-6 R5.	

Mitigation Plan Submitted On: March 20, 2017

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: May 12, 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		
RFC2017016888	07/01/2016	CIP-007-6 R5.

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 R5 – System Access Controls.

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

On 03/01/2016, an internal Annual Vulnerability Assessment conducted the Primary Asset Subject Matter Expert (SME) at [REDACTED] identified four shared accounts on [REDACTED] assets that did not meet CIP-007-6 Part 5.5 password parameter requirements. Shared account password lengths for the [REDACTED]. A total of [REDACTED] users have access to the four shared accounts on the [REDACTED] assets. All of these [REDACTED] people have taken the required NERC training; have had the required background check performed, and possess a need to know.

Per the local [REDACTED] vulnerability management procedure, internal vulnerability assessments are provided to the corporate [REDACTED] group for review and determination of vulnerabilities to [REDACTED] assets/systems. If a vulnerability exists, a ticket is opened (through the [REDACTED] Hotline) and a Remediation Team is used to evaluate the impact on any [REDACTED] assets. If the Remediation Team impact analysis indicates no threat to the [REDACTED] environment, the ticket is updated and closed. If the Remediation Team impact analysis determines the vulnerability impact is "Critical" to [REDACTED] operations, a Remediation ticket will be opened and the Remediate Vulnerability Process will begin. On affected [REDACTED] assets, the responsible Cyber Subject Matter Expert(s) (SMEs) will assume ownership of the identified vulnerability and mitigation.

The internal vulnerability assessment identifying the inadequate shared account passwords was handed off by the [REDACTED] SME to the [REDACTED] group in the second quarter of 2016. A vulnerability review was completed by [REDACTED] on 07/29/2016. However, there was no evidence of a ticket being opened for an impact evaluation nor was there evidence of a ticket being opened to initiate the Remediate Vulnerability process.

The [REDACTED] group discovered the violation during their monthly internal audit of [REDACTED] November 2016 audit randomly sampled [REDACTED] assets, discovered the shared account violation late in the month, and reported the issue to the [REDACTED] on 12/01/2016.

The [REDACTED] verified with the [REDACTED] SME on 12/19/2016 that no mitigation plan was generated for any of the issues identified in the 03/01/2016 [REDACTED] Annual Vulnerability Assessment.

Timeline:

03/01/2016 - [REDACTED] Annual Vulnerability Assessment discovery of [REDACTED] asset shared accounts that violated CIP-007-6 Part 5.5 standards for password parameter requirements.

2nd Quarter 2016 - Annual Vulnerability Assessment handed off from [REDACTED] to [REDACTED] to conduct a review and impact analysis.

07/29/2016 - Vulnerability review was completed by [REDACTED]

12/01/2016 - Discovery of [REDACTED] asset shared accounts violation during routine audit conducted by [REDACTED] group.

12/03/2016 - [REDACTED] brought the [REDACTED] assets into compliance by using [REDACTED]

Cause: (what caused the violation?)

The local [REDACTED] vulnerability management process lacks clarity around [REDACTED] handoffs and does not include escalations when hand-offs do not occur.

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

The [REDACTED] group discovered the violation during their monthly internal audit of [REDACTED] [REDACTED] randomly sampled [REDACTED] assets, discovered the shared account violation late in the month, and reported the issue to the [REDACTED] on 12/01/2016.

Plan Details

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

The action plan will include updating the [REDACTED] vulnerability management process document to clarify [REDACTED] handoffs and include escalations when hand-offs do not occur. The action plan will also include updating System Access Controls Program documentation to address NERC-CIP password parameter standards for shared accounts.

Actions to protect the assets interim, while the mitigation is being implemented:

While mitigating actions are being implemented [REDACTED] will continue to utilize the [REDACTED] ([REDACTED]) process to ensure authorized access to shared accounts are maintained.

Reviewers (Supervisors and Role Owners) conduct quarterly reviews to confirm the appropriateness of user's access to NERC-CIP related accounts - including local accounts (e.g., non-LDAP), shared accounts and group accounts - based on an individual's job function. Any access that has been flagged for removal is forwarded to [REDACTED] ([REDACTED]) in the [REDACTED] ([REDACTED]) who remove the access.

After the [REDACTED] have completed the removals, the [REDACTED] NERC Analyst verifies that all of the "removals" have been completed based on post-removal data extracts provided by the [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: May 12, 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	[REDACTED] Annual Vulnerability Assessment conducted March 2016.	12/09/2016	12/05/2016		No
Milestone 2	Annual Vulnerability Assessment Risk Assessment from [REDACTED] [REDACTED] [REDACTED]	12/09/2016	12/19/2016		No
Milestone 3	Bring shared account passwords for [REDACTED] [REDACTED] assets into compliance with [REDACTED] Standards for	12/09/2016	12/09/2016		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
	password length and complexity requirements and CIP-007-6 Part 5.5 standards for password complexity requirements.				
Milestone 4	Identify all assets containing shared accounts at [REDACTED] and verify they meet NERC CIP-007-6 Part 5.5 standards for password length and complexity requirements.	03/09/2017	03/09/2017		No
Milestone 5	Update [REDACTED] vulnerability management process document to clarify [REDACTED] handoffs and include escalations when hand-offs do not occur.	03/15/2017			No
Milestone 6	Update [REDACTED] NERC- [REDACTED] paragraph 4 "[REDACTED]" to include note that shared accounts must meet NERC-CIP standards for password length and complexity.	04/14/2017			No
Milestone 7	Update System Access Controls Template [REDACTED] worksheet "Procedure for Changing Password" section to include note that shared accounts must meet	04/21/2017			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
	NERC-CIP standards for password length and complexity.				
Milestone 8	████ communication to █████ of new standards and updated standards needs to be formalized to allow █████ to maintain compliance.	04/28/2017			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.

The impact to the BPS is low due to only personnel with the requisite NERC Critical Infrastructure Security Training and NERC CIP Personnel Risk Assessment (background check from HR) have access to shared accounts for the [REDACTED] assets. On 12/03/2016, [REDACTED] brought the [REDACTED] assets into compliance by using [REDACTED]

While implementing this Mitigation Plan, [REDACTED] did not identify any risk or potential impacts, nor does [REDACTED] anticipate any increased risk to the reliability of the bulk power system.

Prevention

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

This mitigation plan will prevent further violations of the same or similar reliability standards in the future by:

- (1) Updating the System Access Controls program documentation to direct that shared accounts meet NERC-CIP standards for password length and complexity.
- (2) Clarifying [REDACTED] vulnerability management process handoffs and including escalations when these handoffs do not occur to ensure the process is followed accurately and in a timely manner.

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

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): RFC2017016888

Mitigated Standard Requirement(s): CIP-007-6 R5.

Scheduled Completion as per Accepted Mitigation Plan: May 12, 2017

Date Mitigation Plan completed: May 19, 2017

RF Notified of Completion on Date: May 26, 2017

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2017016888 Mitigation Certification.zip	File "RFC2017016888 Mitigation Certification.zip" contains: RFC2017016888_Cover Page.pdf - Cover page for whole file Milestone 1 - Submit.pdf - Contains evidence supporting Milestone 1 Milestone 2 - Submit.pdf - Contains evidence supporting Milestone 2 Milestone 3 - Submit.pdf - Contains evidence supporting Milestone 3 Milestone 4 - Submit.pdf - Contains evidence supporting Milestone 4 Milestone 5 - Submit.pdf - Contains evidence supporting Milestone 5 Milestone 6 - Submit.pdf - Contains evidence supporting Milestone 6 Milestone 7 - Submit.pdf - Contains evidence supporting Milestone 7 Milestone 8 - Submit.pdf - Contains evidence supporting Milestone8	8,022,515

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]

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

ReliabilityFirst

[REDACTED]

May 26, 2017

Email: [REDACTED]

Phone: [REDACTED]

Authorized Signature _____ Date _____

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

[REDACTED]

The internal vulnerability assessment identifying the inadequate shared account passwords was handed off by [REDACTED] to [REDACTED] in the second quarter of 2016. A vulnerability review was completed by [REDACTED] on 07/29/2016. However, there was no evidence of a ticket being opened for an impact evaluation nor was there evidence of a ticket being opened to initiate the Remediate Vulnerability Process.

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	RFC2017016888 Mitigation Certification	CIP-007-6 R5
File 2	RFC2017016888-[REDACTED] Response to Additional information requested for Milestone 2 and 7.	CIP-007-6 R5

Verification of Mitigation Plan Completion

Milestone 1: [REDACTED] Annual Vulnerability Assessment conducted March 2016.

File 1, “RFC2017016888 Mitigation Certification”, Milestone 1- Submit, Pages 2 through 16 show the CVA which caught this issue.

Milestone #1 Completion Verified.

Milestone 2: Annual Vulnerability Assessment Risk Assessment from [REDACTED]

This milestone was an attempt to go above and beyond. However, [REDACTED] did not inform [REDACTED] about the deliverable (i.e. the risk assessment). [REDACTED] completed the CVA, but did not complete the risk assessment referenced in the milestone. After the CVA was completed, [REDACTED] made the assessment on what was the most important/critical item to correct (prioritizing action items from the CVA). Though not an official risk assessment, [REDACTED] prioritized the work based on potential security risks identified by the CVA that was conducted by [REDACTED]

Milestone # 2 Completion verified.

Milestone 3: Bring shared account passwords for [REDACTED] [REDACTED] assets into compliance with [REDACTED] Standards for password length and complexity requirements and CIP-007-6 Part 5.5 standards for password complexity requirements.

File 1, “RFC2017016888 Mitigation Certification”, Milestone 3, Pages 2 through 23, show approved change requests/ work order in which to change passwords. Page 25, shows that password complexity requirements have been enabled via Local Security Policies.

Milestone #3 Completion Verified.

Milestone 4: Identify all assets containing shared accounts at [REDACTED] and verify they meet NERC CIP-007-6 Part 5.5 standards for password length and complexity requirements.

File 1, “RFC2017016888 Mitigation Certification”, Milestone 4, Pages 2 through 34, show an inventory of all assets that contain shared accounts at [REDACTED]

Milestone #4 Completion Verified.

Milestone 5: Update [REDACTED] vulnerability management process document to clarify [REDACTED] handoffs and include escalations when hand-offs do not occur.

File 1, “RFC2017016888 Mitigation Certification”, Milestone 5, Page 2, illustrates that a revision has recently been made (2-27-2017) as required by this milestone. In addition Pages 4 through 6, describe the responsibilities of the individual contributors.

Milestone #5 Completion Verified.

Milestone 6: Update [REDACTED] NERC-[REDACTED] paragraph 4 [REDACTED] [REDACTED] to include note that shared accounts must meet NERC-CIP standards for password length and complexity.

File 1, “RFC2017016888 Mitigation Certification”, Milestone 6, Pages 2 through 21, illustrate that on May 17, 2017, that [REDACTED] NERC [REDACTED] was updated to include a segment in regards to shared account complexity and length.

Milestone #6 Completion Verified.

Milestone 7: Update System Access Controls Template [REDACTED] worksheet "Procedure for Changing Password section to include note that shared accounts must meet NERC-CIP standards for password length and complexity.

File 2, "RFC2017016888- [REDACTED] Response to Additional information requested for Milestone 2 and 7", Milestone 2 and 7, Page 10, item 7 shows that the entity has accounted for the changing of default passwords as required by CIP-007-6 and item 7 which describes password complexity which each provide a link to further parts of the document to provide additional detail. Page 11 and 12, show the requirements for entity related password length and complexity.

Milestone #7 Completion Verified.

Milestone 8: [REDACTED] communication to [REDACTED] of new standards and updated standards needs to be formalized to allow [REDACTED] to maintain compliance.

File 1, "RFC2017016888 Mitigation Certification", Milestone 8, Pages 2 through 4, illustrate communication to affected parties that [REDACTED] has updated internal controls, policies, and documents which in addition communicate that password length and complexity requirements have also changed.

Milestone #8 Completion Verified.

The Mitigation Plan is hereby verified complete.

Date: August 16, 2017

A handwritten signature in black ink, appearing to read "Tony Purgar". The signature is fluid and cursive, with the first name "Tony" and last name "Purgar" clearly distinguishable.

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation

Attachment 12

Record documents for the violation of CIP-009-6 R1

- 12.a The Entity's Self-Report (RFC2016016384);
- 12.b The Entity's Mitigation Plan designated as RFCMIT012374 submitted [REDACTED];
- 12.c The Entity's Certification of Mitigation Plan Completion dated [REDACTED];
- 12.d ReliabilityFirst's Verification of Mitigation Plan Completion dated [REDACTED]

Self Report

Entity Name: [REDACTED] ([REDACTED])

NERC ID: [REDACTED]

Standard: CIP-009-6

Requirement: CIP-009-6 R1.

Date Submitted: [REDACTED]

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED] [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: July 01, 2016

End/Expected End Date: October 25, 2016

Region Initially Determined a September 28, 2016
Violation On:

Reliability Functions: [REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]

Is Possible Violation still Yes
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: During the [REDACTED] CIP v5 implementation, [REDACTED] implemented 8 [REDACTED] firewalls, two on 09/01/2015, two on 09/15/2015, two on 09/22/2015, and two on 12/15/2016. These firewalls were in addition to four pre-existing [REDACTED] Firewalls. The intentions for the implementation of the 8 [REDACTED] Firewalls was to divide one Electronic Security Perimeter (ESP) into four separate ESPs. [REDACTED] has a recovery plan (CIP009 Recovery Plan) that requires creation of "Recovery Procedures" by the technology. On 09/28/2016, during an internal review, it was noted that the 8 [REDACTED] firewalls do not have Recovery Procedures as required by the [REDACTED] Recovery Plan.

Mitigating Activities:

Description of Mitigating Mitigating Activities:
Activities and Preventative Develop and implement recovery plans for all [REDACTED] Firewalls (Due on
Measure: 10/24/2016).
Existing Regular backup includes [REDACTED] Firewalls. (On going)
All other applicable controls such as access control, password control, and
patching are effective and up to date since the deployment. (On going)

Self Report

Preventive Measures:

[REDACTED] ([REDACTED]) has been updated to inspect for the deployment of future technologies and to ask question to update the required documentation.(Completed 3/8/2016)

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Severe

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: The actual impact to the BPS is low because [REDACTED] did have vendor specific recovery procedures available in the event of a failure.

Risk Assessment of Impact to BPS: [REDACTED] does not foresee any impact to the BPS due to 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: 1

NERC Violation ID	Requirement	Violation Validated On
RFC2016016384	CIP-009-6 R1.	

Mitigation Plan Submitted On: [REDACTED]

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: November 17, 2016

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		
RFC2016016384	07/01/2016	CIP-009-6 R1.

Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.

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

During the [REDACTED] CIP v5 implementation, [REDACTED] implemented 8 [REDACTED] firewalls, two on 09/01/2015, two on 09/15/2015, two on 09/22/2015, and two on 12/15/2016. These firewalls were in addition to four pre-existing [REDACTED] Firewalls. The intentions for the implementation of the 8 [REDACTED] Firewalls was to divide one Electronic Security Perimeter (ESP) into four separate ESPs. [REDACTED] has a recovery plan (CIP009 Recovery Plan) that requires creation of "Recovery Procedures" by the technology. On 09/28/2016, during an internal review, it was noted that the 8 [REDACTED] firewalls do not have Recovery Procedures as required by the [REDACTED] Recovery Plan.

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

On 09/28/2016, during an internal review, it was noted that the 8 [REDACTED] firewalls do not have Recovery Procedures as required by the [REDACTED] Recovery Plan.

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:

██████ has implemented a change control process that requires the creation of recovery procedures for any new NERC protected assets on 3/8/16. However ██████ firewalls were deployed in December 2015.

Updated process requires an update to be made to the ██████ recovery plan for any new NERC protected assets.

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

Proposed Completion date of Mitigation Plan: November 17, 2016

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

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
Create Recovery procedures	Create Recovery procedures for ██████ devices	10/25/2016	10/25/2016		No
Update Recovery plan	Update Recovery Plan to include ██████ devices	10/28/2016	10/28/2016		No
Update implementation checklist	Update ██████ Checklist to require creation of recovery procedures and updating of the recovery plan for new NERC devices by Asset type	10/28/2016	03/08/2016	This task was in fact completed on 3/8/2016.	No
Verify that no other assets are missing respective Recovery Procedure	Confirm with SMEs that all the assets that need to have a recovery procedure do in fact have a recovery procedure.	11/09/2016			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.

While implementing this Mitigation Plan, [REDACTED] did not identify any risk or potential impacts, nor does [REDACTED] anticipate any increased risk to the reliability of the bulk power system.

Prevention

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

The update of the [REDACTED] checklist, created on 3/8/16, requires recovery plans and recovery procedures to be developed or update whenever there is implementation of a NERC protected asset.

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

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: ██████████

NERC Registry ID: ██████████

NERC Violation ID(s): RFC2016016384

Mitigated Standard Requirement(s): CIP-009-6 R1.

Scheduled Completion as per Accepted Mitigation Plan: November 17, 2016

Date Mitigation Plan completed: November 09, 2016

RF Notified of Completion on Date: ██████████

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	RFC2016016384 Certification Package.zip	The zip file "RFC2016016384 Certification Package.Zip" contains the following files: RFC2016016384 Certification cover page - submit.PDF - This is the coversheet for the whole package Milestone 1 - Submit.PDF - First page of this file is the cover page for this milestone and remaining evidence is bookmarked within. Milestone 2 - Submit.PDF - First page of this file is the cover page for this milestone and remaining evidence is bookmarked within. Milestone 3 - Submit.PDF - First page of this file is the cover page for this milestone and remaining evidence is bookmarked within. Milestone 4 - Submit.PDF - First page of this file is the cover page for this milestone and remaining evidence	8,784,307
Entity	File 2 Firewall Implementation (002).docx		153,134
Entity	File 3 RFC2016016384 MPVR RF Response 2-23-17.docx		22,518
Entity	File 4 RFC2016016384 - Firewall Implementation_June.docx		153,905

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.

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

ReliabilityFirst

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 RFC2016016384

Standard/Requirement: CIP-009-6 R1

NERC Mitigation Plan ID: RFCMIT012374

Method of Disposition: Not yet determined

Relevant Dates					
Initiating Document	Mitigation Plan Submittal	RF Acceptance	NERC Approval	Certification Submittal	Date of Completion
██████████	██████████	██████████	██████████	██████████	11/09/16

Description of Issue

During the █████ CIP v5 implementation, █████ implemented 8 █████ firewalls, two on 09/01/2015, two on 09/15/2015, two on 09/22/2015, and two on 12/15/2016. These firewalls were in addition to four pre-existing █████ Firewalls. The intentions for the implementation of the 8 █████ Firewalls was to divide one Electronic Security Perimeter (ESP) into four separate ESPs. █████ has a recovery plan (CIP009 Recovery Plan) that requires creation of "Recovery Procedures" by the technology. On 09/28/2016, during an internal review, it was noted that the 8 █████ firewalls do not have Recovery Procedures as required by the █████ Recovery Plan.

Evidence Reviewed		
File Name	Description of Evidence	Standard/Req.
File 1	RFC2016016384 Certification Package	CIP-009-6 R1
File 2	Firewall Implementation (002)	CIP-009-6 R1
File 3	RFC2016016384 MPVR RF Response 02-23-17	CIP-009-6 R1
File 4	RFC2016016384 Firewall Implementation June	CIP-009-6 R1

Verification of Mitigation Plan Completion

Milestone 1: Create Recovery procedures for [REDACTED] devices.

File 2, “*Firewall Implementation (002)*”, and File 3, “*RFC2016016384 MPVR RF Response 02-23-17*”, having an email exchange with them and consulting with compliance, and then reviewing file 4, that the [REDACTED] and [REDACTED] [REDACTED] devices are not considered EACMS devices due to them not controlling any devices within the ESP. This seems to be gap within the standards.

Milestone # 1 Completion verified.

Milestone 2: Update Recovery Plan to include [REDACTED] devices.

File 2, “*Firewall Implementation (002)*”, and File 3, “*RFC2016016384 MPVR RF Response 02-23-17*”, having an email exchange with them and consulting with compliance, and then reviewing File 4, “*RFC2016016384 Firewall Implementation June*”, that the [REDACTED] and [REDACTED] [REDACTED] devices are not considered EACMS devices due to them not controlling any devices within the ESP. This seems to be gap within the standards.

It is noted in File 1, “*RFC2016016384 Certification Package*”, Milestone 2 – Submit.pdf that the [REDACTED] firewall devices receive their configuration and configuration changes from the Panorama software server after the initial setup of the [REDACTED]. The “[REDACTED] Firewall Backup, Recovery and Failover Procedures Version1.0” has been created and made part of [REDACTED] set of recovery plans with a signature approval on Page 12 of the Milestone 2 – Submit.pdf.

Milestone # 2 Completion verified.

Milestone 3: Update [REDACTED] Checklist to require creation of recovery procedures and updating of the recovery plan for new NERC devices by Asset type.

File 2, “*Firewall Implementation (002)*”, and File 3, “*RFC2016016384 MPVR RF Response 02-23-17*”, having an email exchange with them and consulting with compliance, and then reviewing File 4, “*RFC2016016384 Firewall Implementation June*”, that the [REDACTED] and [REDACTED] [REDACTED] devices are not considered EACMS devices due to them not controlling any devices within the ESP. This seems to be gap within the standards.

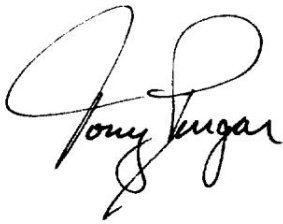
Milestone # 3 Completion verified.

Milestone 4: Verify that no other assets are missing respective Recovery Procedure.

File 2, “*Firewall Implementation (002)*”, and File 3, “*RFC2016016384 MPVR RF Response 02-23-17*”, having an email exchange with them and consulting with compliance, and then reviewing File 4, “*RFC2016016384 Firewall Implementation June*”, that the [REDACTED] and [REDACTED] [REDACTED] devices are not considered EACMS devices due to them not controlling any devices within the ESP. This seems to be gap within the standards.

Milestone # 4 Completion verified.

The Mitigation Plan is hereby verified complete.



Date: [REDACTED]

Tony Purgar
Manager, Risk Analysis & Mitigation
ReliabilityFirst Corporation