

COVER PAGE

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Compliance Exceptions in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see [this document](#).

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	FRCC2019020957	Yes		Yes	Yes									Category 1 – 3 years Category 2 – 12: 2 years
2	MRO2017016816			Yes	Yes					Yes	Yes		Yes	Category 2 – 12: 2 years
3	MRO2018020158	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
4	MRO2018020159	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
5	MRO2018020573	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
6	MRO2018020576	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
7	MRO2018020833			Yes	Yes									Category 2 – 12: 2 years
8	MRO2018020293	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
9	MRO2018019581	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
10	MRO2018020804	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
11	MRO2017017597	Yes		Yes	Yes					Yes				Category 2 – 12: 2 years
12	MRO2018018952			Yes	Yes					Yes				Category 2 – 12: 2 years
13	MRO2018018966			Yes	Yes					Yes				Category 2 – 12: 2 years
14	MRO2018019577			Yes	Yes					Yes				Category 2 – 12: 2 years
15	MRO2018020537	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
16	MRO2018020603			Yes	Yes					Yes				Category 2 – 12: 2 years
17	MRO2018020604			Yes	Yes					Yes				Category 2 – 12: 2 years
18	MRO2018020513			Yes	Yes									Category 2 – 12: 2 years
19	MRO2018020147			Yes	Yes									Category 2 – 12: 2 years
20	MRO2018020671	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
21	MRO2018020696			Yes	Yes									Category 2 – 12: 2 years
22	MRO2018020698			Yes	Yes									Category 2 – 12: 2 years
23	MRO2018019024	Yes		Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 years
24	SPP2017018368			Yes	Yes									Category 2 – 12: 2 years
25	SPP2017018369			Yes	Yes									Category 2 – 12: 2 years

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
26	MRO2018020802	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
27	SPP2018019315			Yes	Yes								Yes	Category 2 – 12: 2 years
28	MRO2018020628	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
29	MRO2017017601	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
30	MRO2018019229	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
31	MRO2018020136	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
32	NPCC2019020907			Yes	Yes									Categories 2– 12: 2 year
33	NPCC2018020277			Yes	Yes									Categories 2 – 12: 2 year
34	NPCC2018019537	Yes		Yes	Yes				Yes					Categories 2 – 12: 2 year
35	NPCC2017018295	Yes		Yes	Yes						Yes	Yes		Category 1: 3 year; Categories 2-12: 2 year
36	NPCC2017018523	Yes		Yes	Yes						Yes	Yes		Categories 2 – 12: 2 year
37	RFC2018020141	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
38	SERC2018019357			Yes	Yes									Category 2 – 12: 2 years
39	SERC2018019921			Yes	Yes									Category 2 – 12: 2 years
40	SERC2018019456			Yes	Yes									Category 2 – 12: 2 years
41	SERC2018019033			Yes	Yes									Category 2 – 12: 2 years
42	TRE2017016871	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
43	TRE2017016875			Yes	Yes						Yes			Category 2 – 12: 2 year
44	TRE2018020488	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
45	TRE2017017145			Yes	Yes									Category 2 – 12: 2 year

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2019020957	CIP-010-2	R1.1.2.	██████████ ("the Entity")	██████████	9/23/2018	9/25/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed noncompliance.)			<p>On January 18, 2019, the Entity submitted a Self-Report stating that, ██████████, it was in noncompliance with CIP-010-2 R1. The Entity failed to authorize and document a change that deviated from the existing baseline configuration.</p> <p>This noncompliance started on September 23, 2018, when firmware upgrade change was implemented without prior authorization and ended on September 25, 2018, when the firmware upgrade change was authorized, and the baseline updated.</p> <p>This issue involves the inadvertent failure to authorize and document a firmware upgrade for one Physical Access Control System (PACS) NERC Integrated Lights-Out (iLO) device and was discovered by a detective control in place to detect changes within one day and resolved on the second day.</p> <p>A firmware upgrade was needed on iLO devices because the old firmware was going to lose support from the vendor. A PowerShell script was run in a corporate subnet that contains corporate Integrated Lights-Out (iLOs) to perform a firmware upgrade on non-NERC devices. ██████████. The script performed as designed and upgraded the firmware of all iLOs in that corporate subnet, including NERC iLO device.</p> <p>Therefore, this device was upgraded without the prior authorization and documentation that is required for applicable devices.</p> <p>An extent of condition review was performed by the Entity and revealed no additional occurrences.</p> <p>The cause for this noncompliance was a gap in a desk level procedure (DLP). The DLP did not require the subject matter expert to confirm that no applicable Cyber Assets would be affected by the PowerShell script that is used to install firmware upgrades.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>The risk of failure to authorize and document a change that deviated from the existing baseline configuration (i.e., this firmware upgrade) could have introduced an unknown change to the environment thereby potentially impacting the PACS device and its ability to maintain security of the physical security perimeter protecting BES Cyber Assets. This could thereby lead to unauthorized physical access and potential impact to the reliability of the BPS.</p> <p>The risk was reduced as the firmware change upgrade being implemented had been tested multiple times on the corporate side and the firmware was from a trusted source. Additionally, the changes to the baseline were promptly detected and authorized. The Entity also performed security validations and found that the firmware posed no threat to the system.</p> <p>The Region determined that the Entity's compliance history should not serve as a basis for applying a penalty. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) took corrective action creating change order to update iLOs firmware; 2) performed an extent of condition review determining the Entity has a total of 280 iLOs. 30 of those iLOs are applicable Cyber Assets and 3 of the applicable Cyber Asset iLOs required this upgrade. Only one of the three resides within the corporate subnet; 3) performed a root cause analysis; 4) added preventative control by adding an additional step to the desk level procedure for assigned team to manually review and determine which Cyber Assets are applicable prior to implementation; and 5) communicated new change in desk level procedure to required team members. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2017016816	CIP-004-6	R5	[REDACTED]	[REDACTED]	08/01/2016	10/14/2016	Compliance Audit	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>During a Compliance Audit conducted from [REDACTED] MRO determined that [REDACTED], was in noncompliance with CIP-004-6 R5. [REDACTED]</p> <p>MRO determined there were three instances of noncompliance with P5.1 and one instance of noncompliance with P5.3. The first instance of noncompliance with P5.1 involved an individual with unescorted physical access who was terminated on July 31, 2016, whose access was not removed within 24 hours, but whose access was removed on August 2, 2016. The second instance of noncompliance with P5.1 involved an individual with unescorted physical access who was terminated on August 2, 2016 and whose access was removed some time on August 3, 2016; [REDACTED] could not demonstrate that the removal took place within the required 24 hours due to the lack of a timestamp. The third instance of noncompliance with P5.1 involved an individual with unescorted physical access who was terminated on October 13, 2016 and whose access was removed some time on October 14, 2016; [REDACTED] could not demonstrate that the removal took place within the required 24 hours due to the lack of a timestamp. The noncompliance with P5.3 involved an individual with access who was terminated on Friday August 12, 2016, whose access was not removed within 24 hours, but whose access was removed on Sunday August 14, 2016.</p> <p>The cause of the noncompliance was inadequate processes to ensure that access was removed within 24 hours and inadequate processes to demonstrate compliance with the 24-hour removal requirement (i.e. no timestamps).</p> <p>The duration of the noncompliance was not contiguous; the noncompliance began sometime on August 1, 2016, 24 hours after the individual in the first instance of noncompliance with P5.1 was terminated, and ended on October 14, 2016 when the physical access for the individual in the third instance of noncompliance with P5.1 was removed.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance did not involve any terminated individuals with electronic access to a High or Medium Impact BES Cyber System or an associated PACS or EACMS device. Additionally, the duration of the individual instances of noncompliance was no greater than 48 hours which significantly reduced the risk. No harm is known to have occurred.</p> <p>MRO reviewed [REDACTED] CIP-004-6 R5 compliance history. [REDACTED] relevant compliance history includes a minimal risk FFT for CIP-004-2 R4 [REDACTED] mitigated on or before August 3, 2010. This noncompliance involved three instances where [REDACTED] failed to promptly revoke physical access; specifically they failed to complete the last step of physical access removal (removal from badge server) within seven days. [REDACTED] also had a minimal risk FFT for CIP-004-3 R4 [REDACTED] that was mitigated on or before March 23, 2012. The noncompliance involved [REDACTED] failing to promptly revoke an intern's physical access after the need ended because the intern's supervisor was on vacation. MRO determined that [REDACTED] compliance history should not serve as a basis for applying a penalty, as the current noncompliance was not caused by a failure to mitigate the prior noncompliance and because of the substantial duration between the prior and current noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) removed all access for the terminated individuals and confirmed that the access was removed; and 2) modified its termination and de-provisioning processes, including the addition of timestamps. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020158	CIP-007-6	R2	[REDACTED]	[REDACTED]	5/16/2018	5/22/2018	self-log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 10, 2018, [REDACTED] submitted a self-log stating that it was in noncompliance with CIP-007-6 R2. [REDACTED]. The noncompliance occurred in [REDACTED]. [REDACTED] states that while updating documentation for security patch installation records, it discovered that six patches had not been timely installed on [REDACTED] Cyber Assets as required by P2.3.</p> <p>The cause of the noncompliance was that [REDACTED] did not follow its documented process to apply patches or develop a patch mitigation plan within 35 days; a newly assigned CIP SME was not familiar with the CIP compliance process and related tools.</p> <p>The noncompliance began on May 16, 2018, 36 days after the patches had been evaluated and deemed applicable, and ended on May 22, 2018, when the patches were applied.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per [REDACTED], the protocols that were subject to the vulnerability were blocked by the firewall, [REDACTED]. Additionally [REDACTED] states that [REDACTED]. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) applied the applicable patches; 2) provided additional training to the responsible CIP SME; 3) the compliance team expanded and modified existing processes and patch tracking documentation to help newly assigned CIP SMEs monitor and install security patches; and 4) the CIP SMEs created documentation that includes responsibilities specific to the security patching process to be used by newly assigned CIP SMEs. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020159	CIP-007-6	R5	██████████	██████████	1/26/2017	6/11/2018	self-log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 10, 2018, ██████████, submitted a self-log stating that it was in noncompliance with CIP-007-6 R5. ██████████. The self-log identified two instances of noncompliance. The noncompliance occurred in ██████████.</p> <p>In the first instance of noncompliance, ██████████ states that during an access review, it discovered a shared user account for an EACMS device was not inventoried as required by P5.2. The cause of the noncompliance was that ██████████ did not follow its documented process on inventorying new accounts. The noncompliance began on January 26, 2017, when the account was created, and ended on May 25, 2018, when the account was inventoried.</p> <p>In the second instance of noncompliance, ██████████ states that during an annual review of BES Cyber Assets and associated accounts, it discovered a user account associated with an EACMS device that did not have its password changed within 15 calendar months as required by P5.6. The cause of the noncompliance was that the user account shared the same name as another documented user account; ██████████ states that during the last password change the SME (who was new to the position) believed that both passwords had been updated when only one had been. The noncompliance began on April 12, 2018, when the password had not been changed in the last 15 months, and ended on June 11, 2018, when the account was deleted.</p> <p>The noncompliance began on January 26, 2017, when the account in the first instance was created, and ended on June 11, 2018, when the account in the second instance was deleted.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk associated with the first instance is minimal because per ██████████, the account is limited to the web interface to configure a server and the account cannot be used to initiate user interactive access to the ESP. Further, ██████████ states that it reviewed logs that demonstrated that the account had only been used once during the initial configuration, and there were no other log in attempts during the period of noncompliance. The risk associated with the second instance is minimal because per ██████████ the device ██████████. Additionally, ██████████ states that it reviewed logs associated with the user account and discovered no suspicious user access during the period of noncompliance. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, ██████████:</p> <p>To mitigate the first instance, ██████████:</p> <ol style="list-style-type: none"> 1) added the account to the inventory; 2) documented a standardized process to ensure that persons who are newly assigned CIP SME responsibilities are adequately informed as to the details of their duties; 3) added additional instructions to the change management tool on the new device workflow to make the task of configuring and documenting accounts more clear and to provide specific direction to inventory application accounts that provide shared interactive user access; and 4) an email regarding the mitigating activities was sent to all affected teams. <p>To mitigate the second instance, ██████████:</p> <ol style="list-style-type: none"> 1) deleted the account; 2) verified that all passwords for local user accounts are managed by a password management tool; 3) documented a standardized process for adding responsibilities to a new CIP SME; and 4) configured the asset tool management application to detect and ensure that passwords are changed. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020573	CIP-006-6	R1	[REDACTED]	[REDACTED]	10/25/2017	07/17/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 5, 2018, [REDACTED] submitted a self-log stating that it was in noncompliance with CIP-006-6 R1. [REDACTED] The noncompliance occurred at the [REDACTED], which is located in [REDACTED].</p> <p>[REDACTED] stated that there was a construction project adjacent to the PSP ([REDACTED]). [REDACTED] stated that the construction project required the creation of an opening on the PSP wall. [REDACTED] reported that the opening was in the wall that separated the [REDACTED] and the PSP, and that the opening was above the ceilings tiles (approximately 12 feet above the ground). [REDACTED] stated that the construction was completed on October 25, 2017, and the integrity of the PSP perimeter was not verified as part of the project completion process. [REDACTED] reported that it discovered the opening on July 16, 2018 during its annual PSP inspection.</p> <p>The cause of the noncompliance was inadequate processes related to construction projects that impact the PSP, specifically, [REDACTED] had no processes to verify its PSP access controls after the completion of a construction project.</p> <p>The noncompliance began on October 25, 2017 when the construction project was completed, and ended on July 17, 2018 when the opening was closed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per [REDACTED] the opening was only accessible from inside the [REDACTED] and access to the [REDACTED] is controlled by electronic card access. Further, [REDACTED] stated that the opening was not visible as it was covered by ceiling tiles, and that accessing the PSP via the opening would have required the use of a ladder and the removal of ceiling tiles while in full view of security cameras. [REDACTED] reported that an investigation indicated that there was no unauthorized physical access via the opening and that there were no unauthorized electronic access attempts for the [REDACTED] Cyber Assets located in the PSP during the period of the noncompliance. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) closed the opening in the wall above the ceiling; 2) modified its project initiation and commissioning forms to include additional information for projects impacting PSPs and a physical security walkthrough at the end of all PSP projects; and 3) the project management business unit held a team meeting to review and enforce the new processes and forms. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020576	CIP-007-6	R2	[REDACTED]	[REDACTED]	5/3/2018	6/14/2018	self-log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 5, 2018, [REDACTED], submitted a self-log stating that it was in noncompliance with CIP-007-6 R2. [REDACTED]. The noncompliance occurred in [REDACTED].</p> <p>[REDACTED] states that during an internal audit, it discovered that it did not assess patches for applicability at least every 35 days for [REDACTED] BES Cyber Assets. The devices were deployed on November 15, 2017, [REDACTED] states that at that time the software was updated and baselines were created for the devices. However, the SME who documented the baseline, failed to add the devices to the tool that is used for assessing and tracking patch applicability. As a result, [REDACTED] failed to consistently assess patches for applicability that were released for these [REDACTED] BES Cyber Assets.</p> <p>The cause of the noncompliance was that [REDACTED] did not follow its documented process to update the device inventory during deployment.</p> <p>The noncompliance began on May 3, 2018, 36 days after the last evaluation, and ended on June 14, 2018, when the patches were assessed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per [REDACTED], the noncompliance was limited to two BES Cyber Assets, the noncompliance lead to 12 patches that were released on [REDACTED] to not be timely assessed for applicability, upon assessment only four of the 12 patches were deemed to be applicable, and those vulnerabilities were classified as low-risk. Additionally, [REDACTED] states that [REDACTED]. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) assessed the patches and applied the applicable patches; 2) added the BES Cyber Assets to the device inventory; 3) sent an email to all CIP SMEs reinforcing the two-step process for replacement of an existing device; and 4) updated the process to replace/retire Cyber Assets. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020833	CIP-010-2	R1	[REDACTED]	[REDACTED]	12/14/17	1/18/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 16, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. Specifically, [REDACTED] failed to update the documented baselines for two Cyber Assets within 30 days as required by P1.3.</p> <p>The cause of the noncompliance was that the task became stalled in the Change Management Process.</p> <p>This noncompliance started on December 14, 2017, 31 days after the approved change was made to the two Cyber Assets and ended on January 18, 2018, when the baselines were updated.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was minimal because per [REDACTED] the scope of the noncompliance was limited two Cyber Assets. Additionally, [REDACTED] states that the noncompliance was able to be resolved through the updating of documentation only and that the change had been tested prior to being authorized by [REDACTED]. No harm is known to have occurred.</p> <p>[REDACTED] does not have any relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) updated the baseline for the two Cyber Assets; 2) instituted bi-monthly reminders to prevent stalls in the process; and 3) retrained the applicable team members on the Change Management Process. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020293	CIP-007-6	R5	[REDACTED]	[REDACTED]	12/1/2017	12/8/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On August 7, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5. Specifically, [REDACTED] did not change the passwords for [REDACTED] PACS devices at least every 15 months. [REDACTED] discovered the noncompliance in December 2017 during its annual password change campaign.</p> <p>The cause of the noncompliance is that [REDACTED] did not follow its process. [REDACTED] states the process was not followed because during the 2016 annual password change campaign (which also occurred in December), a SME did not change the passwords for the [REDACTED] PACS devices because the passwords had just been changed on August 30, 2016, and the SME thought the passwords did not need to be changed again during the password change campaign.</p> <p>This noncompliance started on December 1, 2017, 15 months after the passwords were changed, and ended on December 8, 2017, when the passwords were changed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per [REDACTED] the scope of the noncompliance was limited, [REDACTED] has over [REDACTED] Cyber Assets and the noncompliance only impacted [REDACTED] of them. Additionally, the duration of the noncompliance was brief. No harm is known to have occurred.</p> <p>MRO considered [REDACTED] relevant compliance history. [REDACTED] CIP-007-6 R5 compliance history includes noncompliance with CIP-006-3a R2 [REDACTED] that was resolved as a moderate risk violation. The prior noncompliance involved a failure to apply a broad range of cyber security controls, including annual password change, to PACS devices. MRO determined that [REDACTED] compliance history should not serve as a basis for applying a penalty. MRO determined that the current noncompliance was not caused by a failure to mitigate the prior noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) changed the passwords; 2) provided reinforcement training to the applicable SME; 3) had the team responsible for managing passwords implement a peer-review process as part of the annual password change campaign; and 4) had the compliance and quality control teams perform quality check reviews as part of the annual password change campaign. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019581	CIP-007-6	R4	[REDACTED]	[REDACTED]	07/01/2016	01/22/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 10, 2018, [REDACTED] submitted a self-log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R4. Specifically, [REDACTED] had BES Cyber Assets that were not configured to log successful and unsuccessful logins as required by P4.1. [REDACTED] states that it discovered the noncompliance during preparation for its 2017 vulnerability assessment. [REDACTED] reports that it completed an extent of conditions review for similar noncompliance in all substations that contain medium impact BES Cyber Assets. Per [REDACTED] it discovered that [REDACTED] BES Cyber Assets (relays) were not configured to log successful login attempts as required by P4.1.1, and that [REDACTED] of those [REDACTED] were also not configured to log unsuccessful login attempts as required by P4.1.2.</p> <p>The cause of the noncompliance was weakness in [REDACTED] process that did not include specific direction to verify that the device had been configured to enable logging.</p> <p>The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on January 22, 2018 when all the relays were configured to enable logging.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] states that the relays were part of BES Cyber Systems that did not have External Routable Connectivity. [REDACTED] reports that it applied CIP Cyber Security controls to the relays and the substations that house the relays that are above the requirements of the CIP Standards. Specifically, [REDACTED] states that physical access to the substation is protected by [REDACTED], and that [REDACTED] applied [REDACTED] to the relays that went above the requirements of [REDACTED]. Further, the scope of the noncompliance is limited ([REDACTED]). No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) configured all relays to enable logging; 2) added a row to the QA Settings Review to verify necessary logging; and 3) developed a job aid to identify all models capable of logging. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020804	CIP-007-6	R2	[REDACTED]	[REDACTED]	7/1/2016	7/11/2018	self-log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 9, 2018, [REDACTED] submitted a self-log stating that it was in noncompliance with CIP-007-6 R2. The self-log identified four instances of noncompliance. [REDACTED] stated that it discovered the noncompliance during a periodic review of documentation.</p> <p>The first instance of noncompliance involved a failure to identify a patch source for a PACS device. Specifically, the patch source for the firmware on a server's network card was not identified as required by P2.1. The noncompliance began on July 1, 2016, when the standard became enforceable, and ended on June 7, 2018 when the patch source was identified and evaluated.</p> <p>The second instance of noncompliance involved a failure to identify a patch source for a PACS device. Specifically, the patch source for a server's anti-virus application was not identified as required by P2.1. The noncompliance began on January 9, 2018, when the application was installed, and ended on April 9, 2018 when the patch source was identified and evaluated.</p> <p>The third instance of noncompliance involved a failure to identify a patch source for a PACS device. Specifically, the patch source for a server's intrusion detection application was not identified as required by P2.1. The noncompliance began on January 9, 2018, when the application was installed, and ended on April 9, 2018 when the patch source was identified and evaluated.</p> <p>The fourth instance of noncompliance involved a failure to apply two applicable patches on a PACS device. Specifically, two patches were not applied to a server within 35 days of evaluation as required by P2.3 due to a miscommunication between two departments. The noncompliance began on January 24, 2018, 36 days after the patches were evaluated, and ended on July 11, 2018 when the patches were applied.</p> <p>The cause of the noncompliance was that [REDACTED] did not follow its process to identify patch source or install patches after evaluation.</p> <p>The noncompliance began on July 1, 2016, when the standard became enforceable, and ended on July 11, 2018, when the patches in the fourth instances were applied.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The first, second, and third instance were minimal because per [REDACTED], no security patches were released during the period of noncompliance. The fourth instance was minimal because per [REDACTED], the noncompliance only impacted a single server, the server is logically isolated from BES Cyber Systems, [REDACTED]. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) identified the patch sources and evaluated the patch sources for the first three instances; 1) applied the patches in the fourth instance; 3) augmented the change management process to include more direction to document patch sources; and 4) had the compliance department establish a monthly internal control to monitor the patch source report. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2017017597	CIP-007-6	R4	[REDACTED]	[REDACTED]	2/22/2017	3/9/2018	Self-Log	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)</p>			<p>On [REDACTED] submitted a self-log to MRO stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2. [REDACTED] Subsequently, during a Compliance Audit that occurred between [REDACTED], MRO determined that there were two additional instances of noncompliance with CIP-007-6 R4. MRO later determined that the description in the self-log did not constitute noncompliance.</p> <p>For the first instance of noncompliance, during the Compliance Audit, two of ten sampled Cyber Assets (PCAs) were unable to provide evidence (logs) of successful and unsuccessful logins as required by P4.1. A post-audit extent of conditions analysis discovered an additional [REDACTED] Cyber Assets [REDACTED] EACMS, [REDACTED] PCAs) that could not provide evidence of successful and unsuccessful logins. The noncompliance impacted devices that were associated with [REDACTED]. The cause of the noncompliance was that [REDACTED] failed to follow its documented process related to configuring logging. The noncompliance began on February 22, 2017 when an error was made during the Active Directory reconfiguration, and ended on March 9, 2018 when it confirmed the authentication events were being logged.</p> <p>For the second instance of noncompliance, during the Compliance Audit, [REDACTED] of 28 sampled Cyber Assets were unable to provide evidence that a sample of logs were reviewed at least every 15 days as required by P4.4. MRO determined that the review of logs were all missed for all Cyber Assets within the same period of time. The noncompliance impacted devices that were associated within the [REDACTED]. The cause of the noncompliance was that [REDACTED] failed to assign personnel to handle this review during the planned absence of applicable staff. The noncompliance began on March 19, 2017 when the logs of the Cyber Assets were not reviewed at least every 15 days, and ended on March 24, 2017 when a sample of logs were reviewed.</p> <p>The noncompliance began on February 22, 2017 when an error was made during the Active Directory reconfiguration in the first instance, and ended on March 9, 2018 when it confirmed the authentication events were being logged in the first instance.</p>					
<p>Risk Assessment</p>			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The first instance of noncompliance was minimal because per [REDACTED] the Cyber Assets were still logging for detected malicious code (P4.1.3) and [REDACTED]. The second instance was minimal because MRO determined that all the Cyber Assets were reviewed within 20 days. Additionally, per [REDACTED] this represented a single incident out of 200 review periods. Finally, [REDACTED] states that a [REDACTED]. No harm is known to have occurred.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, [REDACTED]</p> <p>To mitigate the first instance of noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) conducted an extent of conditions analysis; 2) resolved the Active Directory configuration error to enable logging on the [REDACTED] Cyber Assets; 3) reviewed procedures for changing and testing group policy changes; and 4) emphasized the importance of security monitoring to the relevant team. <p>To mitigate the second instance of noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) reviewed the sufficiency of existing processes and procedures; 2) modified the applicable procedure to ensure that the results of the review is discussed during a reoccurring meeting; 3) reviewed the standard with and emphasized the importance of security monitoring to the relevant team; and 4) conducted training on the updated procedure for the relevant resources. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018018952	CIP-004-6	R5	[REDACTED]	[REDACTED]	06/09/2017	08/23/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 16, 2017, [REDACTED] submitted a self-log to MRO stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5. [REDACTED] The noncompliance occurred [REDACTED]. The self-log identified two instances.</p> <p>The first instance involved the removal of access for a resigning employee as required by P5.1. [REDACTED] states that a [REDACTED] employee with physical access to two Control Centers resigned on June 8, 2017. [REDACTED] reports that the employee surrendered the badge to security personnel who locked it in a desk drawer. [REDACTED] states that the employee's supervisor did not timely submit a revocation form and that access was not removed in the system until June 9, 2017; the removal was not within 24 hours of the resignation as required by P5.1.</p> <p>The second instance involved the removal of access for a retiring employee as required by P5.3. [REDACTED] states that a [REDACTED] employee retired on August 16, 2017 and had physical and electronic access to BES Cyber System Information. [REDACTED] states that the employee's supervisor did not timely submit a revocation form and that access was not removed until August 23, 2017.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The first instance was minimal risk because, per [REDACTED], the duration of the noncompliance was less than one day, the employee's badge was locked in a desk during the noncompliance, and a review of access logs confirmed the badge was not used during the noncompliance. The second instance was minimal risk because, per [REDACTED], the duration of the noncompliance was less than one week, a review of access logs confirmed the employee's badge or user id was not used during the noncompliance. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) revoked the access for both employees; and 2) issued a ""counseling letter"" to the supervisor in the second instance to reinforce the importance of timely submissions. <p>The mitigating activities [REDACTED].</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018018966	CIP-014-2	R5	[REDACTED]	[REDACTED]	05/29/2016	06/10/2016	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 16, 2017, [REDACTED] submitted a self-log to MRO stating that, as a [REDACTED] it was in noncompliance with CIP-014-2 R5. [REDACTED] The noncompliance occurred [REDACTED]</p> <p>During an internal assessment of CIP-014-2, [REDACTED] identified a date discrepancy between the completion of R2 and R5. Under the Standard, [REDACTED] was required to develop a physical security plan (R5) within 120 days of the completion of the third-party verification (R2). [REDACTED] identified that [REDACTED] physical security plan was not completed within 120 days of the third-party verification.</p> <p>The cause of the noncompliance was that [REDACTED] process used NERC implementation timeline guidance (that contained "not later than" dates), rather than calculating the required dates.</p> <p>The noncompliance began on May 29, 2016, 121 days after the third-party verification (R2) and ended on June 10, 2016, when the physical security plan was developed.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] states that it developed its physical security plan earlier than the "no later than" guidance posted by NERC. Further, the duration of the noncompliance was limited to 12 days. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) updated its documented process to include the proper timeline calculation; and 2) successfully followed the updated process with [REDACTED] most recent CIP-014-2 R1 assessment. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019577	CIP-010-2	R1	[REDACTED]	[REDACTED]	8/1/2017	3/28/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 10, 2018, [REDACTED] submitted a self-log to MRO stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. [REDACTED] The noncompliance occurred [REDACTED].</p> <p>Specifically, [REDACTED] stated that during a port scan, it discovered that the baseline for [REDACTED] Cyber Assets was incomplete. [REDACTED] reports that it switched the maintenance of the ports and services portion of the baseline from one team to another. [REDACTED] states that when this change was made, the relevant process was not updated to include the step to forward the ports and services baseline change to the new team.</p> <p>The noncompliance was caused by a lack of detail in the process, specifically a lack of detail about updating the new team about ports and services baseline changes.</p> <p>The noncompliance began as early as August 1, 2017, when the ports and services baseline data base was deployed, and ended on March 28, 2018, when the baselines for all Cyber Assets was updated.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] states that the noncompliance was limited to updating the baselines and that all the enabled ports and services were necessary. Additionally, [REDACTED] reports that the noncompliance impacted less than [REDACTED] of its substation Cyber Assets. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) updated the Cyber Assets' baselines; and 2) realigned the process to ensure that proper communications take place. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020537	CIP-004-6	R5	[REDACTED]	[REDACTED]	04/12/2018	08/16/2018	Self-Log	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)</p>			<p>On October 10, 2018, [REDACTED] submitted a self-log to MRO stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5. [REDACTED] The noncompliance occurred [REDACTED]. The self-log identified three issues.</p> <p>The first issue involved the removal of access for transferring employees as required by P5.2. [REDACTED] states that an employee transferred jobs, the employee's new manager performed the review, and determined on June 19, 2018 that the access was no longer necessary and should be removed. Per [REDACTED] states that on June 21, 2018, the manager followed up with security personnel who discovered that the removal had not been completed and that the [REDACTED] immediately removed the access. Per [REDACTED] it completed an investigation that determined a coding error [REDACTED]. [REDACTED] reports that it conducted an extent of condition analysis and determined that three employees who should have had access removed on April 12, May 12, and May 16, 2018 retained access as a result of the same coding error. [REDACTED] The cause of the noncompliance was a coding error in the software. The noncompliance began on April 12, 2018, when an employee's access was not timely removed and ended on June 22, 2018 when all four employees' access was removed.</p> <p>The second issue involved the removal of access for a retiring employee as required by P5.1. [REDACTED] states that an employee with electronic access to an EACMS system retired on June 30, 2018; the EACMS system impacted the [REDACTED]. [REDACTED] states that the manager timely submitted the revocation request in the [REDACTED] but there was a delay in processing revocations in its access revocation tool. [REDACTED] reports that the noncompliance was detected on July 2, 2018 through a weekly reconciliation meeting that reviewed discrepancies between the [REDACTED]. The cause of the noncompliance was that [REDACTED] experienced a software issue and did not verify that the revocation was timely performed. The noncompliance began on July 1, 2018, when an employee's electronic access was not timely removed and ended on July 2, 2018 when all the employee's electronic access was removed.</p> <p>The third issue involved the removal of access for an employee that resigned as required by P5.1. [REDACTED] states that an [REDACTED] with physical access resigned on August 12, 2018, but the employee's manager did not submit the removal request until August 14, 2018. [REDACTED] reports that the removal was routed to a security officer who did not have the authority to remove unescorted physical access, who marked the removal to be completed by another security officer with such authority. [REDACTED] states that the noncompliance was detected on August 16, 2018 through a report issued by its system. The cause of the noncompliance is that [REDACTED] failed to follow its revocation process and the revocation was routed to an individual that did not have the authority to complete the revocation. The noncompliance began on August 13, 2018, when an employee's physical access was not timely removed and ended on August 16, 2018 when the physical access was removed.</p> <p>The noncompliance was not contiguous; the noncompliance began on April 12, 2018, when an employee in the first issue did not have the access timely removed, and ended on August 16, 2018, when the access for the employee in the third issue was removed.</p>					
<p>Risk Assessment</p>			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first issue was minimal risk because per [REDACTED], none of the employees had electronic access to a Cyber Asset. Additionally, [REDACTED] that the employees were current employees, were current on CIP training and had valid Personnel Risk Assessments (PRA). Further, [REDACTED] confirmed that none of the badges were used to access a PSP during the period of noncompliance. No harm is known to have occurred.</p> <p>The second issue was minimal risk because per [REDACTED], the Cyber Assets which the employee still had electronic access to could not be accessed through a direct connection from the Internet, and [REDACTED]; [REDACTED] states that the retired employee did not have access [REDACTED] during the period of noncompliance. Further, the retired employee was current on CIP training and had a valid PRA. Finally, [REDACTED] confirmed that the retired employee did not log onto the Cyber Assets during the period of noncompliance. No harm is known to have occurred.</p> <p>The third issue was minimal risk because per [REDACTED], the employee's badge was taken upon the resignation becoming effective and was secured in the manager's officer during the period of noncompliance. Additionally, [REDACTED] states that the former employee was not terminated for cause, did not have logical access to a Cyber Asset, was current on CIP training, and a had a valid PRA. No harm is known to have occurred.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020537	CIP-004-6	R5	[REDACTED]	[REDACTED]	04/12/2018	08/16/2018	Self-Log	Completed
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <p>To mitigate the first issue of noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) removed the transferred employees' access; 2) performed a manual review of all identified removals during the time the coding error was being corrected; and 3) worked with its vendor to correct the coding error. <p>To mitigate the second issue of noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) removed the retired employee's access. 2) reviewed the future effect dates in the access management system; 3) has committed to continue a weekly termination reconciliation process [REDACTED]; and 4) [REDACTED]. <p>To mitigate the third issue of noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) removed the former employee's physical access; 2) coached the former employee's manager on the importance of timely access removal requests; and 3) revised its process to allow any operator to disable badges and remove physical access. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020603	CIP-002-5.1	R1	[REDACTED]	[REDACTED]	9/1/2016	7/19/2018	self-log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 10, 2018, [REDACTED], submitted a self-log to MRO stating that, [REDACTED], it was in noncompliance with CIP-002-5.1 R1. [REDACTED] The noncompliance occurred [REDACTED].</p> <p>Specifically, [REDACTED] failed to identify each asset that contains a low impact BES Cyber System as required by P1.3. [REDACTED] states that there is a jointly owned substation in which [REDACTED] owns one-third of the 115 kV substation facilities. [REDACTED] reports that it incorrectly believed that it only owned the distribution assets at the substation and therefore removed the associated low impact BES Cyber Systems on its P1.3 documentation.</p> <p>The noncompliance was caused by incorrect one-line drawings that did not accurately identify the joint ownership of the Facility</p> <p>The noncompliance began on September 1, 2016, when the substation was removed from its P1.3 documentation, and ended on July 19, 2018, when the substation was added back to the P1.3 documentation.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The substation had no medium or high impact BES Cyber Systems and [REDACTED] confirmed that the substation was on the joint owner's P1.3 documentation and that the other joint owner was compliant with CIP-003-7 R2. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) added the substation to its P1.3 documentation and corrected the one-line diagram; and 2) conducted a full review of contracts to identify other joint ownership facilities. <p>Mitigation was limited to the [REDACTED].</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020604	CIP-006-6	R2	[REDACTED]	[REDACTED]	08/14/2018	08/14/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 10, 2018, [REDACTED] submitted a self-log to MRO stating that, as a [REDACTED] it was in noncompliance with CIP-006-6 R2. [REDACTED] The noncompliance occurred [REDACTED].</p> <p>[REDACTED] states that on August 14, 2018, security personnel responded to a door alarm and identified an individual entering the data center PSP without a badge. The security personnel determined that the individual was an unescorted contractor. [REDACTED] states there were two contractors that were installing chiller pipes under the supervision of a third contractor (with authorized physical access) who was acting as the escort; one contractor would measure and cut the pipes outside of the data center and the other one would install the pipes. [REDACTED] states that it asked the contractors to leave the premises pending investigation. [REDACTED] reports that a review of video footage demonstrated that the escort contractor left twice to check equipment or use the restroom, leaving the other contractors unescorted for a total of 11 minutes over a ten-hour period.</p> <p>The cause of the noncompliance was that the contractor with authorized access failed to follow [REDACTED] documented process regarding continuous escort.</p> <p>The noncompliance began on August 14, 2018 when the contractor stopped the continuous escort and ended later that same day when the contractor resumed the escort.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] states that security personnel quickly responded to the door alarm that demonstrates situational awareness. Additionally, per [REDACTED] the contractors did not have electronic access to the BES Cyber Assets located in the data center. Finally, per [REDACTED], the data center was under video surveillance and a review of the footage demonstrated that the contractors' activities were consistent with the work they were contracted to perform. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) requested that the contractors leave the premises pending investigation after the escorting contractor returned and resumed the escort; 2) placed the contractor's badge on watch status so that security personnel would be alerted if the contractor attempted to gain access while the investigation was pending; and 3) requested that the contract firm provide CIP training to any individual who will be working at [REDACTED] facilities. <p>The mitigating activities [REDACTED].</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020513	CIP-004-6	R3	████████████████████	████████	8/2/2018	8/3/2018	self-log	Expected April 1, 2019
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 5, 2018, ██████████ submitted a self-log stating that it was in noncompliance with CIP-004-6 R3. Specifically, ██████ failed to ensure that an individual with authorized unescorted physical access had a personnel risk assessment completed (PRA) within the last seven years. Per ██████, the PRA expired and ██████ discovered the noncompliance through a bi-weekly access report review.</p> <p>The cause of the noncompliance was that ██████ did not follow its process to renew existing PRAs.</p> <p>The noncompliance began on August 2, 2018, when the individual's PRA expired, and ended on August 3, 2018, when the access was disabled.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. ██████ states the employee did not have electronic access to a BES Cyber System. Additionally, ██████ stated that the employee did not access a PSP during the period of noncompliance. Finally, ██████ reports that the employee is in good standing and that ██████ re-granted the access after a successful PRA update. No harm is known to have occurred.</p> <p>While the mitigation is ongoing, ██████ will reduce the risk by continuing to utilize the access report review, a detective control that detected this instance of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, ██████:</p> <ol style="list-style-type: none"> 1) disabled the employee's access pending PRA renewal; 2) conducted training on the PRA renewal process to employees responsible for performing the PRA renewal; and 3) reviewed the bi-weekly access notification process to identify improvements that will assist in PRA renewals. <p>To mitigate this noncompliance, ██████ will complete the following mitigation activity by April 1, 2019.</p> <ol style="list-style-type: none"> 1) create an additional email notification outside of the bi-weekly report that will identify upcoming PRAs that are close to expiration. <p>The reason for the duration of the mitigating activities is due to personnel changes in the group responsible for implementing the activities.</p>					

Midwest Reliability Organization (MRO)

Compliance Exception

CIP

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020147	CIP-004-6	R5	██████████	██████████	1/17/2018	1/31/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 10, 2018, █████ submitted a self-log stating that, as a █████, it was in noncompliance with CIP-004-6 R5. Specifically, █████ failed to revoke a transferred employee's access by the end of the next calendar day as required by P5.2. █████ reports that on January 15, 2018 compliance personnel were notified that an employee no longer required access to a medium impact substation. █████ states that the revocation process was not promptly initiated and the access was not revoked until January 31, 2018.</p> <p>The cause of the noncompliance was a failure to follow its process; the process was not followed because an employee failed to create a ticket for the revocation.</p> <p>The noncompliance began on January 17, 2018, when the access was not revoked by the end of the next calendar day, and ended on January 31, 2018 when the access was revoked.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. █████ reports that the employee is still employed in good standing with █████. Additionally, the employee still had a valid personnel risk assessment (PRA) and was up-to-date on CIP training. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, █████</p> <ol style="list-style-type: none"> 1) revoked the employee's access; and 2) implemented a compliance software tool workflow to codify its process for granting/changing access. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020671	CIP-007-6	R5	[REDACTED]	[REDACTED]	9/8/18	10/2/18	self-log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 10, 2018, [REDACTED] submitted a self-log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5. [REDACTED] states that during a quarterly review of passwords, it discovered that two BES Cyber Assets (RTUs) that were located in substations, had passwords that were not changed within 15 months as required by P5.6.</p> <p>The noncompliance was caused by a lack of detail in the process for updating passwords.</p> <p>This noncompliance started on September 8, 2018, 15 months after the last password change and ended on October 2, 2018, when the passwords were changed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] states that to remotely access the RTU, a user would [REDACTED] prior to being able to attempt access to the RTU with the expired password. Additionally, [REDACTED] reports that it confirmed that all RTU users had authorized CIP access. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) changed the passwords; 2) changed the process related to password changes; and 3) provided training to applicable staff. 					

Midwest Reliability Organization (MRO)

Compliance Exception

CIP

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020696	CIP-004-6	R4	████████████████████	████████	7/1/2016	6/18/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 10, 2018, █████ submitted a self-log stating that, as a █████, it was in noncompliance with CIP-004-6 R4. █████ states that during the cyber vulnerability assessment it identified that a user group had unauthorized local login access to CIP workstations. The user group predated the CIP workstations and inherited local login access when the workstations were added to the domain.</p> <p>The cause of the noncompliance was █████ failure to follow its access management process and it was not knowledgeable about the local domain inheritance policy when the workstations were joined to the domain.</p> <p>The noncompliance began on July 1, 2016, when the standard became enforceable, and ended on June 18, 2018 when the group policy was modified to deny access.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. █████ reports that the user group did not have remote access to the workstations meaning that to utilize the access, the users would have to be credentialed in the PACS system to gain access. █████ also states that all 13 users in the group had valid and up to date personnel risk assessments (PRA) and CIP training. Further, █████ reports that 11 of the 13 members have identical access through their other authorized means and the two remaining users are trusted employees who are CIP Standard Owners who have CIP compliance responsibility. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, █████</p> <ol style="list-style-type: none"> 1) modified the local group policy to deny access for the user group; and 2) reconfigured the CIP database to provide limited access to a group of specific users. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020698	CIP-009-6	R2	[REDACTED]	[REDACTED]	7/1/2018	7/18/2018	self-log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 10, 2018, [REDACTED] submitted a self-log stating that, as a [REDACTED], it was in noncompliance with CIP-009-6 R2. Specifically, [REDACTED] failed to test its recovery plan at least once every 36 months as required by P2.3. [REDACTED] states that it discovered the noncompliance on July 2, 2018 during an annual internal standard review.</p> <p>The cause of the noncompliance was a failure to follow its process; the process was not followed due to a schedule setting error, [REDACTED] entered the process reminders for 2019 instead of 2018.</p> <p>The noncompliance began on July 1, 2018, when the recovery plan was not tested at least once every 36 months, and ended on July 18, 2018 when the recovery plan was tested.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] promptly detected the noncompliance, which limited the duration of the noncompliance to less than 20 days. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) tested the recovery plan; and 2) updated the scheduler reminder to reflect the new recovery plan testing time. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019024	CIP-004-6	R4	██████████	██████████	4/1/2017	6/18/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On November 17, 2017, █████ submitted a Self-Report stating that, as a █████, it was in noncompliance with CIP-004-6 R4. Specifically, █████ failed to verify in the first quarter of 2017 that individuals with access have authorization records as required by P4.2. The late review was completed on June 18, 2017.</p> <p>The cause of the noncompliance was a failure to follow its process; the process was not followed as a result of a miscommunication between two employees.</p> <p>The noncompliance began on April 1, 2017, when the first quarter of 2017 ended without a verification being conducted, and ended on June 18, 2017 when the verification was conducted.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. █████ states that when the late review was performed, all required authorization records were found to be correct. No harm is known to have occurred.</p> <p>MRO considered █████ relevant compliance history. █████ CIP-004-6 R4 compliance history includes noncompliance with CIP-004-1 R4 █████ that was resolved as a minimal risk Find, Fix, Track Report that was mitigated on January 11, 2012. The prior noncompliance involved a failure to include all relevant devices and accounts in the quarterly review. MRO determined that █████ prior noncompliance should not serve as a basis for imposing a penalty. MRO determined that the current noncompliance was not caused by a failure to mitigate the prior noncompliance and the two instances were separated by a substantial duration of time.</p>					
Mitigation			<p>To mitigate this noncompliance, █████</p> <ol style="list-style-type: none"> 1) completed the review; 2) assigned a supervisory task to the CIP-004 Standard Owner to ensure that each portion of the quarterly review occurs prior to the deadline; and 3) created an █████ reminder to remind personnel to perform quarterly reviews. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017018368	CIP-003-6	R2	[REDACTED]	[REDACTED]	4/1/2017	10/30/2018	Spot Check	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>As the result of a Spot Check conducted on September 22, 2017, MRO determined that [REDACTED], as a [REDACTED], was in noncompliance with CIP-003-6 R2. [REDACTED] did not implement its cyber security plans before the standard became enforceable. [REDACTED] jointly owns a single substation with associated low impact BES Cyber System(s). [REDACTED] states that the joint owner registered entity has supervisory control over the substation and [REDACTED] assumed that the other registered entity had assumed all CIP obligations.</p> <p>The cause of the noncompliance is that [REDACTED] did not understand its responsibilities under the standard.</p> <p>This noncompliance started on April 1, 2017, when the standard became enforceable, and ended on October 30, 2018, when [REDACTED] implemented the cyber security plans required by the standard.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] jointly owns a single BES substation and has no supervisory control over any BES Cyber Systems. No harm is known to have occurred.</p> <p>[REDACTED] has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) drafted the necessary procedures; and 2) provided training on the procedures so that it could implement its cyber security plans. <p>MRO verified completion of the mitigation.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017018369	CIP-003-6	R1	[REDACTED]	[REDACTED]	4/1/2017	6/29/2018	Spot Check	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>As the result of a Spot Check conducted on September 22, 2017, MRO determined that [REDACTED], as a [REDACTED], was in noncompliance with CIP-003-6 R1. [REDACTED] did not create cyber security policies required by P1.2 before the standard became enforceable. [REDACTED] jointly owns a single substation with associated low impact BES Cyber System(s). [REDACTED] states that the joint owner registered entity has supervisory control over the substation and [REDACTED] assumed that the other registered entity had assumed all CIP obligations.</p> <p>The cause of the noncompliance is that [REDACTED] did not understand its responsibilities under the standard.</p> <p>This noncompliance started on April 1, 2017, when the standard became enforceable, and ended on June 29, 2018, when [REDACTED] created the cyber security policies required by P1.2 and had it CIP Senior Manager approve the policies.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] jointly owns a single BES substation and has no supervisory control over any BES Cyber Systems. No harm is known to have occurred.</p> <p>[REDACTED] has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) created the cyber security policies required by P1.2; and 2) had it CIP Senior Manager approve the policies. <p>MRO verified the completion of the mitigation.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020802	CIP-010-2	R1	[REDACTED]	[REDACTED]	3/27/2017	9/27/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 8, 2018, [REDACTED] submitted a self-log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. Specifically, for [REDACTED] Cyber Assets, [REDACTED] failed to include all enabled logical ports in its baseline as required by P1.1.4. [REDACTED] reports that two enabled ports on [REDACTED] relays of the same model were not included in the baseline. [REDACTED] states that it discovered the noncompliance when an analyst was performing cyber security controls testing.</p> <p>The noncompliance was caused by a deficiency in [REDACTED] process of evaluating and identifying open ports during commissioning.</p> <p>This noncompliance started on March 27, 2017, when the first relay was placed in-service and ended on September 27, 2018, when the baselines were updated.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per [REDACTED] the relays are configured to allow connectivity with the ports at issue only to specific down-level devices. Additionally, [REDACTED] states that one of the undocumented ports was a port that cannot be disabled per the device capability and the other undocumented port was required for normal operation. Finally, [REDACTED] states that an extent of conditions review confirmed that the noncompliance was limited to [REDACTED] three Cyber Assets. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) performed an extent of conditions to search for similar noncompliance; 2) updated the baselines; 3) implemented a new Cyber Asset security assessment criteria to be used when all new equipment is installed into a substation containing medium impact BES Cyber Systems; and 4) provided training regarding the impact that varying equipment configurations can have on cyber security. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2018019315	CIP-004-6	R4	[REDACTED]	[REDACTED]	7/31/2017	2/2/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 28, 2018 [REDACTED] submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-004-6 R4. [REDACTED] identified two instances of noncompliance with CIP-004-6 R4.</p> <p>The first instance of noncompliance involved an employee who had unauthorized electronic access to multiple newly released EACMS devices associated with a high impact BES Cyber System. [REDACTED] states that the employee required electronic access to configure these devices, and that the employee's access was not authorized because the employee's name was accidentally omitted from a batch authorization form related to the EACMS devices. The cause of the noncompliance was [REDACTED] failure to follow its process for batch authorizing electronic access; the cause for the duration of the noncompliance was that the [REDACTED] quarterly review process lacked sufficient detail, resulting in the unauthorized access not being detected in the third quarter review. The noncompliance began on July 31, 2017 when the EACMS devices were deployed into the production environment, and ended on January 29, 2018 when the employee's electronic access was authorized.</p> <p>The second instance of noncompliance involved an employee who had unauthorized electronic access to an EACMS device associated with a medium impact BES Cyber System at a Transmission Facility. The noncompliance involved an employee who assumed the duties of a resigning employee without first being authorized for that electronic access. [REDACTED] stated that it detected the noncompliance during a review to confirm that it had properly removed the access from the resigning employee. The cause of the noncompliance was [REDACTED] failure to follow its process for granting and authorizing electronic access. The noncompliance began on January 3, 2018 when the employee was granted electronic access to the EACMS, and ended on February 2, 2018 when the employee's electronic access was authorized.</p> <p>The noncompliance began on July 31, 2017, when the EACMS devices in instance one were placed into production, and ended on February 2, 2018, when the electronic access for the employee in instance two was authorized.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In both instances, [REDACTED] stated that they had knowledge the employee had electronic access and the electronic access was proper; thus the noncompliance can accurately be described as a failure to appropriately document the authorization. Additionally, in both instances, per [REDACTED] both employees were current with their CIP training and had a current Personal Risk Assessment (PRA). Further, in the first instance, the employee did not utilize the access during the period of the noncompliance. Finally, in the second instance, the duration of the noncompliance was relatively short. No harm is known to have occurred.</p> <p>[REDACTED] relevant history of noncompliance includes a non-serious and non-substantial violation of CIP-004-1 R4 [REDACTED]. The prior noncompliance involved incomplete electronic access lists ([REDACTED] did not include sufficient detail in its access records) and the noncompliance was mitigated on April 30, 2010. MRO determined that [REDACTED] compliance history should not serve as a basis for applying a penalty. The current noncompliance was not caused by a failure to mitigate the prior noncompliance, and the current and prior noncompliance are separated by a substantial duration of time.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) authorized the electronic access for both employees; 2) revised its procedures for granting/authorizing access and for conducting quarterly reviews; and 3) trained applicable staff on the updated procedures. <p>MRO verified the completion of the mitigating activities.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020628	CIP-010-2	R1	[REDACTED]	[REDACTED]	2/15/2017	3/1/2017	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 5, 2017, [REDACTED] submitted a self-log stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R1. [REDACTED] later submitted an updated self-log on May 22, 2017.</p> <p>[REDACTED] stated it made a change to an antivirus application without receiving authorization for the change. The change impacted the baseline of 27 Cyber Assets (ten high impact BES Cyber Assets, one PACS, ten PCAs and four EACMS devices associated with a [REDACTED] BES Cyber System; and one PACS and one EACMS device associated with a medium impact BES Cyber System). [REDACTED] stated that the SME requested authorization for the change but applied that change on February 15, 2017, prior to the change being authorized; the change was authorized on March 1, 2017.</p> <p>The cause of the noncompliance was a lack of clarity in the process, which led to confusion on the part of the SME.</p> <p>The noncompliance began on February 15, 2017, when the SME made the unauthorized change, and ended on March 1, 2017, when the change was authorized.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was minimal because, per [REDACTED] the change had been tested in the non-production environment prior to being applied and the noncompliance was corrected by processing the formal authorization. Further, the noncompliance was relatively brief (14 days). No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) approved the change request; and 2) improved its process for baseline authorizations, incorporated a unique change task for baseline authorizations to reduce confusion and incorporated a color-coded text to help clarify if a particular task had been updated. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2017017601	CIP-007-6	R1	[REDACTED]	[REDACTED]	7/1/2016	8/7/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On May 16, 2017, [REDACTED] submitted a Self-Report to MRO stating that, as a [REDACTED] it was in noncompliance with CIP-007-6 R1. [REDACTED]. The noncompliance impacted [REDACTED] devices associated with a firewall management system (a system used for managing [REDACTED] that functioned as an EACMS). [REDACTED] states the noncompliance involved [REDACTED] devices where two ports were required to be enabled, but the documentation lacked the need or justification for the two enabled ports. [REDACTED] reports that it documented the ports by March 15, 2017. [REDACTED] states that it discovered the noncompliance during an internal compliance assessment.</p> <p>The cause of the noncompliance is that [REDACTED] procedure for enabling only ports that have been determined to be needed and the corresponding documentation justifying the need was not sufficiently detailed.</p> <p>The noncompliance began on July 1, 2016, when the Standard and Requirement became mandatory, and ended on August 7, 2017, when [REDACTED] documented the need for all required and enabled ports, and updated its procedure regarding the documentation of enabled ports.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a substantial risk to the reliability of the bulk power system. The ports in question were verified to be required for operation, thus the noncompliance was limited to the failure to document that need. Additionally, per [REDACTED] the devices' role as an EACMS was limited to [REDACTED]. No harm is known to have occurred.</p> <p>[REDACTED] has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) conducted an assessment to determine all required ports for the impacted devices; 2) documented the need for all required and enabled ports for the devices; and 3) reviewed and updated its CIP-007-6 procedures to include the required steps in documenting required ports and services. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019229	CIP-010-2	R3	[REDACTED]	[REDACTED]	7/1/2017	8/10/2017	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On January 10, 2018 [REDACTED] submitted a self-log to MRO stating that, as a [REDACTED] it was in noncompliance with CIP-010-2 R3. [REDACTED] The noncompliance impacted [REDACTED] devices associated with a firewall management system (a system used for managing [REDACTED] that functioned as an EACMS).</p> <p>[REDACTED] states that on July 21, 2017, it discovered that it had not conducted a vulnerability assessment on this system that met all subparts of the requirement. Specifically, [REDACTED] stated that automated scans on the system were conducted on January 10, 2017 and January 24, 2017, but those scans did not include all [REDACTED] devices that were part of the system, did not address ports and services reviews, and did not develop an action plan to remediate any identified vulnerabilities (P3.4).</p> <p>The cause of the noncompliance is that [REDACTED] failed to follow its documented processes.</p> <p>The noncompliance began on July 1, 2017, which was the effective date for the Standard and Requirement under the Phased-In Implementation Plan and ended on August 10, 2017 when the vulnerability assessment was conducted.</p>					
Risk Assessment			<p>The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] stated that the vendor of the system hardens the system by removing all hardware and software not essential to the associated tasks, which reduces the attack surface of the devices. Additionally, per [REDACTED] the devices' role as an EACMS was limited to [REDACTED]. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) performed a complete vulnerability assessment; and 2) implemented an automated task in its compliance software to ensure that the system's owner performs the required vulnerability assessment within the required time frame. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020136	CIP-010-2	R2	[REDACTED]	[REDACTED]	11/15/2017	11/21/2017	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 10, 2018, [REDACTED] submitted a self-log stating that as a [REDACTED] it was in noncompliance with CIP-010-2 R2. [REDACTED] stated that on November 21, 2017, it discovered that its baseline verification tool had a coding error that impacted its Cyber Assets associated with its [REDACTED] BES cyber systems, including Windows and network BCAs, PCAs, EACMS, and PACS [REDACTED]. The baseline verification consists of two components: the first component performs the validation of the baseline against a daily scan, which it prompts from the second component; the second component performs the daily scan. A software change that impacted the first component resulted in it being unable to prompt the daily scans from the second component. [REDACTED] stated that the coding error resulted in the verification being performed against an old version (October 10, 2017) of its daily scan results. [REDACTED] reported that it quickly corrected the error.</p> <p>The cause of the noncompliance was that [REDACTED] failed to verify that its technical implementation of its baseline monitoring process was working correctly after a software change in the tool.</p> <p>The noncompliance began on November 15, 2017, 36 days after its last successful baseline comparison and ended later on November 21, 2017, when [REDACTED] performed a new baseline scan and comparison.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per [REDACTED] the noncompliance lasted six days. Additionally, [REDACTED] states that no unauthorized changes were detected in the November 21, 2017 scan. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) corrected the configuration issue and performed a baseline; and 2) implemented a [REDACTED]. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019020907	CIP-006-6	R1.	[REDACTED]	[REDACTED]	12/14/2018	12/21/2018	Self-Report	03/31/2019
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 09, 2019, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it had discovered on December 17, 2018 it was in noncompliance with CIP-006-6 R1. (1.8.) after investigating security footage related to an issue identified by security operations.</p> <p>This noncompliance started on December 14, 2018, when the entity failed to log the entry of an individual with authorized unescorted physical access into one (1) Physical Security Perimeter. The noncompliance ended on December 21, 2018 when the entity terminated the two contractors involved and permanently removed access.</p> <p>Specifically, CIP role-based training expired for a cleaning contractor (Contractor #1) and their access to a Control Center (CC) was automatically deactivated through the physical access system. At the time of the event, Contractor #1's training was compliant with the NERC CIP 15 month requirement, but was not compliant with the entity's 12-month requirement which caused their card access to automatically deactivate. Contractor #1's ID card remained active; only CIP restricted area access was deactivated.</p> <p>Contractor #1 attempted to enter the CC main door three times with the deactivated card and was denied entry each time. At this time, the entity's CIP group personnel received three "Deactivated Card Attempt" emails indicating that Contractor #1 was attempting to access the CC with a deactivated ID card. A few minutes later, Contractor #1 gained access to the CC by using an ID card and associated PIN belonging to a second cleaning contractor (Contractor #2).</p> <p>Approximately one hour later, the security department received a call from Contractor #1 notifying them that they would be opening a door to remove garbage from within the CC; the security department acknowledged this notification. As usual, the opening of the door generated an automated email alert that went to both CIP group and security personnel. CIP Group personnel emailed the security department and requested they identify the individual who had accessed the door.</p> <p>On December 17, 2018, CIP group personnel reviewed the security video footage and determined that Contractor #1 had entered and exited the CC and had utilized the ID card and associated PIN of Contractor #2 to do so. CIP group personnel requested that the facilities department review the events with the two contractors and their supervisor.</p> <p>On December 21, 2018, the facilities department conducted interviews to determine the timeline of the events that occurred. The facilities department requested that security be present and assist with the interviews. A CIP group member was also present for the interviews and provided relevant information. Upon completion of the interview, Contractor #1 and Contractor #2 were no longer allowed to work at the entity's facilities and their access was permanently removed.</p> <p>The root cause of this noncompliance was the failure of two of the individuals to abide by the entity's physical security policy.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to follow the entity's physical security policy and providing another employee physical access to a physical security perimeter, the individual entering the physical security perimeter may not be logged, may not have proper authorization records, and the unescorted access could result in a BES Cyber System being rendered unavailable, degraded, or misused.</p> <p>The risk of the noncompliance was reduced due to the individual previously having authorized access to the CC. The entity's training requirement has a stricter time frame than the standard which resulted in the automated removal of the individual's access. Video footage showed that the individual only utilized access to perform cleaning duties within the CC. Additionally, the entity internally discovered the issue and were able to investigate and mitigate in a short timeframe.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) Permanently removed the two contractors' access to the entity's facilities 2) Included the security department on email distributions for deactivated card alerts at the CC main door. 3) Implemented a process for the security to verify that personnel who notify them regarding door access are already successfully in the CC and logged as such in the log 4) Translated the contractor training to Spanish. 5) Investigated posting a 24 hour guard at the CC main entrance 6) Reminded all employees and sponsors of contractors with unescorted access of the entity's physical security access control procedure. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018020277	CIP-004-6	R4.	[REDACTED]	[REDACTED]	10/01/2016	03/31/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 28, 2018, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on June 1, 2018, it was in noncompliance with CIP-004-6 R4. (4.2.) after a routine evidence review.</p> <p>This noncompliance started on October 1, 2016, the first day after the end of the first quarter of the standard's enforceable date. The entity failed to verify at least once each calendar quarter that individuals with active electronic access had authorization records. The noncompliance affected four (4) EACMS. The noncompliance ended on March 31, 2018, when the entity performed quarterly reviews.</p> <p>The root cause of this noncompliance was a misclassification of the EACMS. The devices were originally classified as an information repository.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, failure to review authorization records of individuals with physical or electronic access to applicable systems could result in unauthorized access or integrity issues of the provisioning system going unnoticed. If unauthorized access was granted to the EACMS in scope, an individual would have access to BES Cyber System Information and could use the sensitive device information to attack critical BES Cyber Systems.</p> <p>The entity reduced the risk of an unauthorized individual using information from the EACMS to gain unauthorized access to its BES Cyber Systems by performing quarterly reviews on its High Impact BES Cyber Systems. The entity also has configuration monitoring in place that would detect changes that include new access or changes to access rights and it would trigger a review. The EACMS in scope are located within Physical Security Perimeters that require two-level authentication to gain physical access.</p> <p>After discovering the issue, the entity performed a review of access and found that all personnel with access to the EACMS assets were authorized to have access. No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> Performed a review of authorization records for individuals with active electronic access or unescorted physical access to the EACMS in scope. <p>To prevent future occurrences, the entity:</p> <ol style="list-style-type: none"> Performed a review of all High Impact BES Cyber Assets and their certification status to ensure no other discrepancies existed. Updated its CIP-010 procedure to determine whether provisioning/access reviews are required for new assets. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019537	CIP-004-6	R2.	[REDACTED]	[REDACTED]	12/01/2017	01/15/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 17, 2018, [REDACTED] (the entity) submitted a Self-Log stating that as [REDACTED] it had discovered on January 5, 2018 it was in noncompliance with CIP-004-6 R2. (2.3.) after reviewing an anomalies report and identifying that several employees had expired training dates without a revocation of access.</p> <p>This noncompliance started on December 1, 2017 when the entity failed to require twenty-one (21) employees complete the training specified in CIP-004-6 R2.1 at least once every 15 calendar months. The 21 employees had physical access to one (1) Medium Impact BES Cyber System with External routable connectivity as well as one area that contains other BES Cyber Systems and Low Impact Electronic Access Points that require procedural physical access controls. The noncompliance ended on January 15, 2018 when the entity had the individuals complete the training or revoked access.</p> <p>Specifically, twelve (12) employees' training expired on December 1, 2017, and nine (9) employees' training expired on January 1, 2018. The involved employees' did not have electronic or information access to BES Cyber Systems (BCS). According to card reader access logs, 13 of the 21 employees entered the PSP (including one who also entered a Physical Security Area that contained associated Cyber Assets and Low Impact Electronic Access Points that do not require a PSP) following the expiration of their training. The entity's system typically sends a revocation email two weeks prior to the expiration of the 15 month CIP-004 training requirement to a revoke group (including security), but that email failed to send.</p> <p>The root cause of this noncompliance was lack of a control to require completion of the training specified in CIP-004-6 R2.1.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not ensuring individuals with unescorted physical access renew their training, the individuals may not be aware of updates to processes regarding physical access controls, visitor controls, cyber security policies, recovery and cyber security risk associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media. This could lead to individuals accessing BES Cyber Systems without a full understanding of responsibilities and the risk associated with their access privileges.</p> <p>Although twenty-one (21) employees were not trained in a timely manner (exceeding the annual training requirement by 9 to 42 days), they were previously provided with cyber security training on multiple occasions and have full understanding of their roles and responsibilities associated with physical access privileges to the PSP. Previous training for the involved employees included NERC CIP training (provided in 2016 after CIP Version 5) and [REDACTED] required cyber awareness training for 2017. Moreover, all of these employees had physical access to only one Physical Security Perimeter (PSP), [REDACTED]. These employees have active PRAs and had no electronic or information access to the BCS.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1. Addressed the non-compliance with training frequency for the twenty-one (21) identified employees: <ol style="list-style-type: none"> a. Completed the required training for sixteen (16) employees on January 9 and 10, 2018 and one (1) completed the training on January 15, 2018. b. Revoked access to four (4) employees <p>To prevent recurrence, the entity:</p> <ol style="list-style-type: none"> 1. Published a user manual to provide formal guidance to staff for managing access rights. 2. Provided user training to all personnel involved in requesting, approving, reviewing, and revoking unescorted physical access or electronic access to BES Cyber Systems/Assets. The training provided clear direction to the entity's supervisors and personnel about timely completion of training where required for legal/regulatory compliance (such as NERC Reliability Standards). 3. Assigned staff to monitor and report on an anomalies review, and escalate concerns to ensure access rights are managed in a timely manner. 4. Developed a process report to record and review anomalies within the system 5. Updated current procedure to include a control for reviewing the anomalies within the system. 6. Provided awareness of the new/revised procedure and to the roles and responsibilities associated with system messaging monitoring. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018295	CIP-007-6	R5.	[REDACTED]	[REDACTED]	07/01/2016	12/29/2017	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED], [REDACTED] (the entity) submitted a Self-Log stating that as [REDACTED] it had discovered on [REDACTED] it was in noncompliance with CIP-007-6 R5. (5.7.) while preparing for an audit.</p> <p>This noncompliance started on July 1, 2016 when the entity failed to submit TFEs for four EACMS that are unable to limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. The four EACMS are associated with two High Impact BES Cyber Systems. The noncompliance ended on December 29, 2017, when the entity upgraded the switches to have the functionality of locking out after meeting a threshold of unsuccessful attempts.</p> <p>The root cause of this noncompliance was a lack of oversight. Specifically, the entity did not have an administrative design to identify standards that had the TFE language instead of the per cyber asset capability language. The entity misinterpreted the standard and thought a manual review of the logs was sufficient to meet the requirement for assets that were not capable.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not limiting or alerting unsuccessful authentication attempts, any attempt to gain unauthorized access to the EACMS could go unnoticed, and an attacker may gain unauthorized access.</p> <p>The entity reduced the risk of an attacker gaining unauthorized access to the devices and brute force password attacks going unnoticed. [REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) Upgraded the switches to have lockout capability. 2) Reviewed the network configuration to explore if the local event logs can be sent to a central Syslog and a SIEM/SOC. The result was unsuccessful. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation or Completion Date
NPCC2017018523	CIP-010-2	R4.	[REDACTED]	[REDACTED]	09/22/2017	10/19/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED], [REDACTED] (the entity) submitted a Self-Report stating that as [REDACTED] it had discovered on [REDACTED], it was in noncompliance with CIP-010-2 R4. On [REDACTED] the entity discovered an additional instance of noncompliance. Both instances were discovered while preparing for an audit.</p> <p>The noncompliance started on September 22, 2017, when the entity failed to implement its documented plan for two Transient Cyber Assets (TCA). Specifically, the entity disclosed username and password information during the initial TCA validation process. A photograph of the laptop was taken as evidence that it had a user account login with password authentication. The photograph showed a label on the laptop with the user name and password. The photograph was made available to staff reviewing the TCA validation evidence package. This noncompliance ended on October 19, 2017 when the entity removed the label, discarded the photograph evidence, and changed the passwords.</p> <p>The root cause of this noncompliance was a failure to follow documented policy. Specifically, the entity's IT and CIP policies state not to write down the password, but personnel did not follow this policy.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not following documented procedures and leaving the username and password on the TCA, an unauthorized individual could gain access to the TCAs which, when connected, could lead to misuse of a BES Cyber System.</p> <p>The entity reduced the risk of an unauthorized individual gaining access to the TCAs by keeping the TCAs locked in the maintenance supervisor's office when they are not in use. [REDACTED] [REDACTED] The entity also performs regular AV and patching on the TCAs in scope which includes verification of asset management system record, so the entity would identify if a laptop had been stolen. The entity also provides cyber security awareness training and site tailgates to address the appropriate authorized use and protection of TCAs.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no relevant underlying causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) Changed the password for the Two TCA's in scope 2) Reviewed classification of the TCA's 3) Conducted training session with the TCA custodians to ensure the log-in credentials are not shared with other personnel <p>To prevent recurrence, the entity:</p> <ol style="list-style-type: none"> 1) Reinforced staff roles and responsibilities to ensure users disconnect transient devices, both physically and logically, from a BES network or device upon task completion. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020141	CIP-007-6	R2	[REDACTED]	[REDACTED]	6/27/2018	7/11/2018	Self-Report	4/30/2019
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 25, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2.</p> <p>The entity is owned and operated by a parent company. While performing the monthly patch review cycle and reviewing the patch evidence for the previous month, the parent company's IT staff identified a required security patch that it failed to install the previous month on one device - [REDACTED]. The patch was required to be installed by June 27, 2018, but the entity failed to install the patch until July 11, 2018, which was 14 days late.</p> <p>The entity performed an investigation and discovered that the required patch was correctly initiated for deployment, but was not installed within the required 35-day period. During the patch installation process, the entity initiated a reboot of the device based on the completion of another patch installation, which inadvertently caused the installation of the patch at issue to be cancelled. The entity IT Subject Matter Expert (SME) responsible for patch installation did not detect that the patch at issue had failed to install after the device rebooted. The IT SME also failed to follow up and verify that the patch had successfully installed.</p> <p>This noncompliance involves the management practices of verification, work management, and workforce management. Verification is involved because the IT SME failed to verify that the patch had successfully installed. The entity lacked an effective process to validate that all patches were successfully installed as intended. That failure to verify is a root cause of this noncompliance. Workforce management is involved because the entity IT SME was not properly trained on how to verify that each patch was successfully installed.</p> <p>This noncompliance started on June 27, 2018, when the entity was required to install the patch at issue and ended on July 11, 2018, when the entity installed the overdue patch.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is that applying this patch 14 days late increases the opportunity for vulnerabilities that could provide a larger attack surface via the unpatched device. The risk is minimized because the device that had the patch installed late [REDACTED] is part of the entity's virtual environment and is not directly connected to any Electronic Security Perimeter (ESP). [REDACTED] Additionally, no web browsing is permitted from the [REDACTED] and that further minimizes the risk. The entity also quickly detected and corrected this noncompliance.</p> <p>No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because of the different causes for the prior noncompliance and for the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity will complete the following mitigation activities by April 30, 2019:</p> <ol style="list-style-type: none"> 1) conducted a quarterly spot check to ensure patch review and implementation is being properly conducted; 2) determined a strategy for providing additional support for patching of IT assets, including third party providers; 3) developed a second level review process specific to [REDACTED] that validates that all patches were deployed correctly; 4) will develop a job aid for the patch review process to facilitate proper monthly evaluation and completion; and 5) will re-train all staff involved in the patch process including the plant and IT management on how to properly conduct a monthly patch review. <p>Prior to completion of the Mitigation Plan, entity SMEs have implemented measures to verify that all intended patches were installed and deployed as expected.</p> <p>The entity needs additional time to be able to retrain all staff.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019357	CIP-006-6	R2.1	[REDACTED]	[REDACTED]	10/23/2017	11/2/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On March 5, 2018, [REDACTED] (the entity) submitted a Self-Report stating that, as [REDACTED] and [REDACTED], it was in noncompliance with CIP-006-6 R2.1.</p> <p>On November 2, 2017, an employee (escort) escorted two contractors into the control center Physical Security Perimeter (PSP). The escort exited the control center equipment room multiple times, leaving the contractors unattended inside the PSP for a total of approximately 20 of 108 minutes the contractors were there. The noncompliance ended on November 2, 2017 when the contractors and their escort exited the PSP for the final time.</p> <p>There were two other instances of this same noncompliance occurring that were discovered in an Extent of Condition (EOC) review. One was on October 23, 2017, when while escorting two contractors within the entity's data center PSP, an employee (escort) left one of the contractors unattended in the equipment room of the PSP when he and the second contractor exited one door from the equipment room of the PSP into the IT Lab room of the PSP for approximately 8 seconds.</p> <p>The other noncompliance took place on November 1, 2017, when while escorting two contractors within the data center PSP, an employee (escort) left both of the contractors unattended in the equipment room of the PSP when he exited the equipment room of the PSP into the IT Lab room of the PSP to retrieve a trash can for approximately 9 seconds.</p> <p>The root cause of this noncompliance and those discovered in the EOC review was a lack of proper training and guidelines for properly escorting visitors within a PSP.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although the contractors were left unattended intermittently during their time in the PSP, the time periods were short, and the escort remained within the PSP very near the contractors. In addition, in all three instances, the contractors and their companies were known to the entity, the contractors were properly logged, and the escorts remained within the PSP nearby the contractors. No known harm occurred because of these issues of noncompliance.</p> <p>Regional Entity determined that the entity's compliance history should not serve as a basis for applying a penalty.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> Had its CIP Senior Manager, and Vice President, IT and Chief Security Officer send an email message to all personnel and contractors with unescorted physical access to a PSP, providing guidelines for properly escorting visitors within a PSP. Incorporated the guidelines into a training curriculum for PSP Escorts. The training was launched on April 30, 2018, via the entity's Learning Management System (LMS). The employees and contractors with unescorted physical access to a PSP will be required to take the training upon receiving access to the PSP. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019921	CIP-004-6	R5.3			1/1/2017	1/4 /2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On June 25, 2018, (the entity) submitted a Self-Report stating that, as a and , it was in noncompliance with CIP-004-6, R5.3.</p> <p>On December 29, 2016, a contractor was voluntarily terminated, however, the contractor's physical BES Cyber System Information (BCSI) access was not revoked by the end of the next calendar day. As required by the Standard, the contractor's physical access to BCSI storage locations should have been revoked by the end of day December 30, 2016. The ticket for the access revocation indicated that the work had been completed on December 29, 2016. However, upon pulling the system records from the BCSI storage location, it was determined the contractor's access was not actually removed until January 4, 2017. There are two issues that are the root cause of this noncompliance. One was the facility services staff member responsible for performing the work mistakenly closed the ticket, indicating the work was complete before actually completing the work 5 days later. The other was the internal control failed because the Compliance Department did not have access to confirm the access to the BCSI physical storage location had been revoked by the next calendar day and had to rely on the dates documented on the ticket.</p> <p>This noncompliance started on January 1, 2017 when the contractor's physical access was not revoked by the end of that day, and ended on January 4, 2017 when access revocation was completed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). While the access had not been revoked, the entity had retrieved the contractor's badge. The noncompliance was short in duration (4 days) and the entity confirmed the contractor's badge was not used between December 29, 2016 and January 4, 2017.</p> <p>No harm is known to have occurred.</p> <p>Regional Entity determined that the entity's compliance history should not serve as a basis for applying a penalty.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) Revoked the contractor's physical access to the BCSI storage locations on January 4, 2017. 2) Transitioned responsibilities for physical access revocations from the facility services Department to the IT organization on May 15, 2017. 3) Implemented an internal control change on June 19, 2018. The system access records now must be attached to the ticket for evidence of access removal within 24 hours of the employee's termination. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019456	CIP-006-6	R2.2			2/15/2018	11/30/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On March 30, 2018, (the entity) submitted a Self-Report stating that, as and , it was in noncompliance with CIP-006-6, R2.2.</p> <p>On February 15, 2018 a group of high school students were escorted to one of the entity's control center viewing gallery. Before the student's arrival to the center, the security guards were provided with a pre-populated visitor logbook page that listed the name of the expected visitor and the responsible party. After the group's departure, the logbook contained 15 incomplete entries pertaining to the group members' PSP entry and exit times. The root cause of this noncompliance a lack of proper training and guidelines for properly escorting visitors within a PSP.</p> <p>The noncompliance duration was less than 8 hours.</p> <p>On November 30, 2018, the security guard at the entity's control center was unable to log a visitor exit time because a security guard in the corporate office building inadvertently had logged the visitor out 28 minutes earlier. Security video verified the actual 28 minute time gap between when the visitor exit was recorded in the corporate office building log and when the visitor exited the control center PSP. The root cause of this issue was human error where an individual, based on assumptions, concluded that activity steps were completed.</p> <p>The noncompliance duration was less than 30 minutes.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The issue was related to actual scribing of the information into the logbook, and the visitors were continuously escorted by the staff at all time. None of the students were allowed to enter the interior control center and had no access to any Bulk Electric System (BES) Cyber Systems (BCSs), and the issue lasted less than 8 hours.</p> <p>In the second instance, the visitor was continuously escorted during the duration the visit in the control center, is an employee in good standing and has a current Personnel Risk Assessment (PRA). The visitor has also completed the appropriate security training eligible for unescorted physical access to the PSP</p> <p>Regional Entity determined that the entity's compliance history should not serve as a basis for applying a penalty.</p>					
Mitigation			<p>To mitigate this noncompliance the entity:</p> <p>In the first instance:</p> <ol style="list-style-type: none"> 1) Trained its security guards on visitor log procedures and logbooks. 2) Updated the training about physical security perimeter access to include language reminding escorts they have a responsibility for ensuring the visitor they are escorting is logged into the visitor logbook. 3) Completed training for staff and contractors with access to the PSP. <p>In the second instance:</p> <ol style="list-style-type: none"> 1) Counseled the security guard at the corporate office building regarding performing due diligence when logging visitors in the visitor logging tool. 2) Made configuration changes to the visitors logging tool programs and trained the security guards on the tool enhancements. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019033	CIP-006-6	R2.2	[REDACTED]	[REDACTED]	6 /13/2017	12/13/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 23, 2018, [REDACTED] (the entity) submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-006-6, R2.2.</p> <p>On June 13, 2017 an entity staff (Staff Member 1) escorted two members of the local Fire Department into the entity's control center. The control center was designed with an external and an internal PSP each requiring visitor logging. Staff Member 1 first escorted the visitors to the areas in the exterior PSP and then escorted them into the interior PSP. Staff Member 1 failed to log the visitors into the interior PSP's visitor logbook before entry.</p> <p>There were three other instances of noncompliance that were discovered during an extent of condition (EOC) review. One was on November 27, 2017 when a security guard failed to log when a contractor exited the control center which was corrected the following day.</p> <p>The second instance was on December 13, 2017 when a contractor was not logged when entering the interior PSP of the control center. The contractor was properly logged into and out of the control center's exterior PSP, which showed the contractor exiting the exterior PSP at 9:40 am on December 13, 2017.</p> <p>The third instance was on July 17, 2017 when a security guard failed to log a contractor into the interior PSP when entering, but corrected this 6 minutes later.</p> <p>The root cause was of this noncompliance was a lack of proper training and guidelines for properly escorting visitors within a PSP.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). In all instances, the issue was related to actual scribing of the information into the logbook, as the visitors were continuously escorted by staff at all times. The collective duration of the four instances of noncompliance lasted less than 24 hours.</p> <p>Regional Entity determined that the entity's compliance history should not serve as a basis for applying a penalty.</p>					
Mitigation			<p>To mitigate this noncompliance the entity:</p> <ol style="list-style-type: none"> 1) Installed new PSP access point signage at eye level on the doors at all entrances to all interior PSPs on June 30, 2017. This signage specifically states that the visitor log must be completed before entering the PSP. 2) Created and distributed a new procedure to security staff on July 19, 2017, requiring security staff to verbally instruct escorts regarding their responsibility to log visitors into an interior PSP Visitor Logbook before entering the PSP. 3) Assigned new training related to PSP logging responsibilities to applicable staff. This new training reinforces the requirement to log a visitor into an interior PSP Visitor Logbook before entry. 4) Counseled the individual escorts regarding proper visitor logging. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017016871	CIP-007-6	R2.	[REDACTED]	[REDACTED]	8/6/2016	10/12/2016	Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>During a Compliance Audit conducted from [REDACTED], Texas RE determined that [REDACTED] as a [REDACTED] was in noncompliance with CIP-007-6 R2. [REDACTED] subsequently submitted a Self-Report to Texas RE stating that, as a [REDACTED] it had two additional instances of noncompliance with CIP-007-6 R2 discovered by [REDACTED] prior to the Compliance Audit.</p> <p>In the first instance, it was discovered during the Compliance Audit that [REDACTED] timely evaluated one applicable security patch; however, [REDACTED] failed to apply the applicable security patch within 35 calendar days of completing its evaluation, as required by CIP-007-6 R2, Part 2.3. The security patch was applicable to two Cyber Assets classified as EACMS. To end the noncompliance [REDACTED] applied the security patch to one Cyber Asset and removed the affected software from the other Cyber Asset. The duration of this instance was less than two weeks.</p> <p>In the second instance, [REDACTED] failed to implement its documented process for tracking, evaluating, and installing security patches as required by CIP-007-6 R2, Part 2.1. [REDACTED] process requires that manual patch sources be monitored at least every 35 days to identify available patches and evaluate them for applicability. Compliance personnel were reviewing manual patch source records and discovered that one source was not being timely evaluated. Upon discovery of the issue, [REDACTED] reviewed the manual patch source and confirmed no patches were released for the time period at issue. The duration of this instance of noncompliance was less than two months.</p> <p>In the third instance, [REDACTED] failed to implement its documented process for tracking, evaluating, and installing cyber security patches as required by CIP-007-6 R2, Part 2.1. [REDACTED] process requires that manual patch sources be monitored at least every 35 days to identify available patches and evaluate them for applicability. Compliance personnel were reviewing manual patch source records and discovered that for one source the number of days between two evaluations exceeded 35 calendar days. The noncompliance ended when [REDACTED] completed an evaluation of the patch source and determined that no patches had been released since the last evaluation. The duration of this instance was two days.</p> <p>For all three instances, the root cause was insufficient processes and controls to ensure that security patches are identified, evaluated, and applied within the required timeframes. For the first instance, [REDACTED] had an insufficient control to monitor patch application deadlines. [REDACTED] relied on a dashboard in its risk and compliance tool to track security patch application deadlines and the ticket for the security patch at issue was tagged with a status that was not included in the dashboard. For the second instance, [REDACTED] had an insufficient process to track active manual patch sources. When one vendor source stopped releasing patches due to software end-of-life status, [REDACTED] personnel stopped reviewing the patch source. However, the patch source was a documented active source, and [REDACTED] process required monitoring of all documented active sources. For the third instance, [REDACTED] had an insufficient control for monitoring patch management process deadlines. [REDACTED] risk and compliance tool used to track security patches was configured to send deadline notifications to only one email address. The manual patch source at issue was setup to send notifications to the email address of the individual with sole responsibility, and this individual was on vacation with no designated backup to complete the required patching task. To prevent recurrence of the issues, [REDACTED] revised its processes and implemented additional controls to timely identify, evaluate, and apply security patches.</p> <p>This noncompliance started on August 6, 2016, the first day after the 35th calendar day after July 1, 2016, when CIP-007-6 R2 became mandatory and enforceable. The noncompliance ended on October 12, 2016, when the security patch impacting two Cyber Assets was applied. The duration of this noncompliance was approximately two months.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure to timely identify, evaluate, and apply security patches has the potential to affect the reliability of the bulk power system (BPS) in that known vulnerabilities on BES Cyber Systems and their associated Cyber Assets may remain unmitigated for an extended period of time. This risk was reduced based on the following reasons. For the first instance, only two Cyber Assets were impacted. Additionally, the duration of the noncompliance was short, lasting less than two weeks. Finally, the software vulnerability addressed by the applicable security patch was classified as a low severity given the effort required to exploit the vulnerability and the potential impact to affected systems. [REDACTED]</p> <p>[REDACTED] For the second instance, only one Cyber Asset was impacted. Further, [REDACTED] confirmed that no security patches were released for the application for the time period at issue. Finally, the noncompliance was the result of a documentation error. For the third instance, only nine Cyber Assets were impacted. The duration for the noncompliance was short, lasting only two days. Finally, no applicable security patches were released for the time period at issue.</p> <p>No harm is known to have occurred.</p> <p>Texas RE considered [REDACTED] compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017016871	CIP-007-6	R2.	[REDACTED]	[REDACTED]	8/6/2016	10/12/2016	Audit	Completed
			<p>1) completed the evaluation of the manual patch sources;</p> <p>2) applied the security patch to one Cyber Asset and removed the affected software from the second Cyber Asset;</p> <p>3) contacted the vendor to confirm patches were no longer released. and designated the applicable patch source as inactive;</p> <p>4) revised its deadline tracking system to send notifications to a group distribution list instead of a single individual;</p> <p>5) modified the dashboard in the risk and compliance tool to identify all patching statuses;</p> <p>6) created new control reports to monitor patching deadlines, monitor all active sources, and alert personnel of upcoming patch deadlines;</p> <p>7) monitored and analyzed the results of the control reports. No additional changes to the control reports were identified; and</p> <p>8) updated the Security Patch Management process document to include guidance on identification of patch sources and require documentation when no security patches are found during manual source checks.</p> <p>Texas RE has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017016875	CIP-010-2	R2.	[REDACTED]	[REDACTED]	8/6/2016	9/27/2016	Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>During a Compliance Audit conducted from [REDACTED], Texas RE determined that [REDACTED] as a [REDACTED] was in noncompliance with CIP-010-2 R2, Part 2.1. Specifically, [REDACTED] failed to monitor at least once every 35 calendar days for changes to the baseline configuration for two Cyber Assets.</p> <p>In late April of 2016, prior to the enforcement date of CIP-010-2 R2, [REDACTED] discovered that two Cyber Assets classified as Electronic Access Control or Monitoring Systems (EACMS) were not communicating with the baseline monitoring system. [REDACTED] determined a manual step was skipped during the installation of the monitoring software. A series of incident tickets and a change ticket were created to establish communication between the Cyber Assets and the baseline monitoring system; however, the failure to prioritize the incident tickets resulted in [REDACTED] failing to meet the initial performance deadline for CIP-010-2 R2, Part 2.1.</p> <p>The root cause of this noncompliance is that [REDACTED] had insufficient processes to ensure all applicable Cyber Assets were properly set up and compliant with CIP-010-2 R2 by the enforcement date. [REDACTED] process for onboarding new Cyber Assets lacked a control to ensure that certain Cyber Assets requiring manual installation tasks are completed. Additionally, [REDACTED] had an insufficient process for prioritizing and fulfilling incident tickets related to Cyber Assets.</p> <p>The noncompliance started on August 6, 2016, one day following the initial deadline for monitoring changes to the baseline configuration, and ended on September 27, 2016, when [REDACTED] corrected the issue to establish baseline monitoring for the two Cyber Assets at issue.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] failure to timely monitor the baseline configuration of Cyber Assets could result in the missed identification and remediation of unauthorized changes that could, in turn, introduce vulnerabilities to its systems due to not verifying the required CIP-005 and CIP-007 security controls. This risk was reduced by the following factors. First, only two Cyber Assets were impacted. Second, the duration was short, lasting only 52 days. Third, [REDACTED] confirmed that there were no unauthorized changes to the two Cyber Assets during the time period at issue. Fourth, other controls were in place to prevent unauthorized access to the Cyber Assets. Specifically, the domain controllers were being monitored for vulnerabilities and patched during the time of the noncompliance. Lastly, the backup domain controllers were being monitored and could be used in the event of a functional issue with the impacted Cyber Assets.</p> <p>No harm is known to have occurred.</p> <p>Texas RE considered [REDACTED] and its affiliate's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) reinstalled the baseline monitoring software on the two impacted Cyber Assets and established monitoring; 2) updated the incident handling process so that personnel assign a high priority status to incident tickets related to Cyber Assets; 3) implemented a process to monitor the communication status of Cyber Assets in the baseline monitoring tool so that any issues are quickly identified and investigated; and 4) implemented a template in the change management system for onboarding new Cyber Assets that automatically includes tasks for confirming the installation of monitoring software per documented instructions. <p>Texas RE verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018020488	CIP-004-6	R5; Part 5.1	[REDACTED]	[REDACTED]	7/4/2018	7/4/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 1, 2018, [REDACTED] submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R5, Part 5.1. In particular, [REDACTED] failed to remove unescorted physical access for one contractor within 24 hours of a termination action.</p> <p>On July 3, 2018, [REDACTED] was notified by a third-party contractor that one contractor resigned. [REDACTED] process to remove physical access requires notification to two separate departments. Notice was sent to the department responsible for removing physical access to buildings, and the contractor's physical access to the entry of the buildings where the Control Centers reside was promptly removed. However, [REDACTED] failed to notify the department responsible for Physical Security Perimeter (PSP) access to remove the contractor's unescorted physical access to the applicable PSPs within the buildings. The following day, a secondary control that identifies discrepancies for PSP access sent an automated e-mail regarding the contractor at issue to the department that manages PSP access. The contractor's unescorted physical access to the PSPs was later removed, ending the noncompliance.</p> <p>The root cause of the noncompliance was a failure to follow the documented access revocation process. [REDACTED] failed to send notice to all departments responsible for unescorted physical access removal following a termination action.</p> <p>The noncompliance started at 10:20 a.m. on July 4, 2018, 24 hours following notification by the contractor's company that the contractor was no longer employed. The noncompliance ended at 8:51 p.m. on July 4, 2018, when the contractor's unescorted physical access to the PSPs was removed. The duration was approximately 10.5 hours.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The potential risk of the failure to timely remove the ability for unescorted physical access to PSPs following a termination action is that the individual could obtain physical access to BES Cyber Systems post-termination and potentially cause harm to BES Cyber Systems. This risk was reduced based on the following factors. First, the contractor at issue was in good standing with [REDACTED]. Second, [REDACTED] promptly removed the contractor's physical access to the entry of the buildings where Control Centers reside once it became aware of the contractor's termination. Third, the duration of the noncompliance was short, lasting approximately 10.5 hours. Fourth, the contractor did not have electronic access to BES Cyber Systems. Fifth, [REDACTED] reviewed physical access logs to its PSPs and confirmed that no attempted entry was made with the contractor's access badge for the time period at issue. Sixth, [REDACTED] has a secondary control in place that identified discrepancies between personnel in the HR system and personnel with PSP access to detect similar issues. [REDACTED]</p> <p>No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) completed removal of the contractor's unescorted physical access to PSPs; 2) reviewed the physical access revocation process and made enhancements as necessary; and 3) provided awareness training regarding the physical access revocation process to personnel responsible for contractors or employees with Control Center PSP access. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017017145	CIP-007-6	R2.			8/28/2016	8/30/2016	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On March 7, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] it had a potential noncompliance with CIP-007-6 R2. Specifically, [REDACTED] failed to implement its documented process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets, as required by CIP-007-6 R2, Part 2.1.</p> <p>[REDACTED] process requires that manual patch sources be monitored at least every 35 days to identify available security patches and evaluate them for applicability. Compliance personnel were reviewing manual patch sources and discovered that for one source the number of days between two evaluations had exceeded 35 calendar days. The noncompliance ended when [REDACTED] completed an evaluation of the patch source and determined that no patches had been released since the last evaluation. The duration of the noncompliance was two days.</p> <p>The root cause of this noncompliance was insufficient controls for monitoring patch management process deadlines. [REDACTED] risk and compliance tool used to track security patches was configured to send deadline notifications to only one email address. The manual patch source at issue was setup to send notifications to the email address of one employee, and the employee was on vacation with no designated backup to complete the required patching task. To prevent recurrence of the issue, [REDACTED] revised its process to implement additional controls to timely identify, evaluate, and apply security patches.</p> <p>The noncompliance started on August 28, 2016, which is the first day after the 35th calendar day following the previous evaluation. The noncompliance ended on August 30, 2016, when [REDACTED] completed an evaluation of the patch source and determined that no patches had been released since the last evaluation.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure to timely identify, evaluate, and apply security patches has the potential to affect the reliability of the bulk power system (BPS) in that known vulnerabilities on BES Cyber Systems and their associated Cyber Assets may remain unmitigated for an extended period of time. This risk was reduced based on the following reasons. First, only nine Cyber Assets were impacted. Second, the duration of the noncompliance was short, lasting only two days. Finally, no applicable security patches were released for the time period at issue.</p> <p>No harm is known to have occurred.</p> <p>Texas RE considered [REDACTED] compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) completed the evaluation of the manual patch source; 2) revised its deadline tracking system to send notifications to a group distribution list instead of a single individual; 3) created new control reports to monitor patching deadlines, monitor all active sources, and alert personnel of upcoming patch deadlines; 4) monitored the control reports and documented results; and 5) analyzed the results of the control report monitoring. No additional changes to the control reports were identified. <p>Texas RE has verified the completion of all mitigation activity.</p>					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

COVER PAGE

This filing contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Compliance Exceptions in this filing and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see [this document](#).

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	FRCC2018020007			Yes	Yes						Yes			Category 2 – 12: 2 years
2	FRCC2018020777		Yes	Yes	Yes									Category 2 – 12: 2 years
3	FRCC2018020721			Yes	Yes									Category 2 – 12: 2 years
4	FRCC2018020697			Yes	Yes									Category 2 – 12: 2 years
5	MRO2018020297			Yes	Yes					Yes				Category 2 – 12: 2 years
6	MRO2018020300			Yes	Yes					Yes				Category 2 – 12: 2 years
7	SPP2017018654			Yes	Yes					Yes				Category 2 – 12: 2 years
8	MRO2018019027	Yes		Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 years
9	MRO2018019028	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
10	MRO2018020291			Yes	Yes								Yes	Category 2 – 12: 2 years
11	MRO2017018346			Yes	Yes									Category 2 – 12: 2 years
12	MRO2018020294	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
13	MRO2018019105			Yes	Yes									Category 2 – 12: 2 years
14	MRO2018019580	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
15	SPP2017016749			Yes	Yes									Category 2 – 12: 2 years
16	MRO2017017624			Yes	Yes									Category 2 – 12: 2 years
17	MRO2018020629			Yes	Yes									Category 2 – 12: 2 years
18	MRO2018019574			Yes	Yes									Category 2 – 12: 2 years
19	MRO2018020143	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
20	MRO2018018951	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
21	MRO2018020135			Yes	Yes									Category 2 – 12: 2 years
22	MRO2018020148	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
23	MRO2018019023			Yes	Yes					Yes				Category 2 – 12: 2 years
24	SPP2018019304	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
25	SPP2018019320			Yes	Yes				Yes					Category 2 – 12: 2 years
26	SPP2017016900			Yes	Yes									Category 2 – 12: 2 years
27	NPCC2017017595			Yes	Yes							Yes		Category 2 – 12: 2 year
28	NPCC2017017913		Yes	Yes	Yes									Category 2 – 12: 2 year
29	NPCC2017018689			Yes	Yes							Yes		Category 2 – 12: 2 year
30	NPCC2018020482		Yes	Yes	Yes						Yes			Category 2 – 12: 2 year
31	NPCC2018020481			Yes	Yes						Yes			Category 2 – 12: 2 year
32	NPCC2018020483	Yes		Yes	Yes						Yes			Category 2 – 12: 2 year
33	NPCC2018020402			Yes	Yes				Yes					Category 2 – 12: 2 year

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
34	NPCC2018019322			Yes	Yes				Yes					Category 2 – 12: 2 year
35	NPCC2018019498			Yes	Yes	Yes						Yes		Category 2 – 12: 2 year
36	NPCC2018019393			Yes	Yes							Yes		Category 2 – 12: 2 year
37	NPCC2017018893			Yes	Yes									Category 2 – 12: 2 year
38	NPCC2017018101	Yes	Yes	Yes	Yes	Yes								Category 1: 3 years; Category 2 – 12: 2 year
39	NPCC2017017899		Yes	Yes	Yes							Yes		Category 2 – 12: 2 year
40	NPCC2018019394			Yes	Yes							Yes		Category 2 – 12: 2 year
41	NPCC2018019359			Yes	Yes	Yes			Yes			Yes		Category 2 – 12: 2 year
42	NPCC2017017599	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
43	NPCC2017018298	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
44	NPCC2017018296		Yes	Yes	Yes									Category 2 – 12: 2 year
45	NPCC2017018297			Yes	Yes									Category 2 – 12: 2 year
46	NPCC2018019395			Yes	Yes							Yes		Category 2 – 12: 2 year
47	NPCC2017017892		Yes	Yes	Yes									Category 2 – 12: 2 year
48	NPCC2017017893			Yes	Yes									Category 2 – 12: 2 year
49	NPCC2017017894			Yes	Yes									Category 2 – 12: 2 year
50	NPCC2017017896			Yes	Yes				Yes					Category 2 – 12: 2 year
51	NPCC2017017897	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
52	NPCC2017018432			Yes	Yes						Yes			Category 2 – 12: 2 year
53	NPCC2017017914		Yes	Yes	Yes									Category 2 – 12: 2 year
54	NPCC2017018688			Yes	Yes						Yes	Yes		Category 2 – 12: 2 year
55	NPCC2018020575			Yes	Yes									Category 2 – 12: 2 year
56	RFC2018019214			Yes	Yes							Yes		Category 2 – 12: 2 year
57	RFC2017018650			Yes	Yes				Yes					Category 2 – 12: 2 year
58	RFC2015015373	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 year
59	RFC2016015835			Yes	Yes				Yes					Category 2 – 12: 2 year
60	RFC2017017324	Yes	Yes	Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 year
61	RFC2016016354	Yes	Yes	Yes	Yes				Yes		Yes			Category 1: 3 years; Category 2 – 12: 2 year
62	RFC2017017618		Yes	Yes	Yes									Category 2 – 12: 2 year
63	RFC2017018652	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
64	RFC2017017733	Yes	Yes	Yes	Yes	Yes	Yes							Category 1: 3 years; Category 2 – 12: 2 year
65	RFC2018019573	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 year
66	RFC2017018543	Yes	Yes	Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 year

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
67	RFC2017018542	Yes	Yes	Yes	Yes	Yes			Yes					Category 1: 3 years; Category 2 – 12: 2 year
68	RFC2017018477	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 year
69	RFC2017018478		Yes	Yes	Yes		Yes		Yes					Category 2 – 12: 2 year
70	RFC2017018479	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 year
71	RFC2017018480	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 year
72	RFC2018019650	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 year
73	RFC2018019381	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 year
74	RFC2017018863	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 year
75	RFC2017018711	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 year
76	RFC2018019841	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 year
77	RFC2018019405	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 year
78	RFC2018019262	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
79	RFC2017018710	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 year
80	RFC2017018770	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 year
81	RFC2017018772	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 year
82	RFC2018019117	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
83	RFC2018019463	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
84	RFC2018020407	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 year
85	RFC2018020408			Yes	Yes				Yes					Category 2 – 12: 2 year
86	RFC2018020409	Yes		Yes	Yes	Yes	Yes							Category 1: 3 years; Category 2 – 12: 2 year
87	RFC2018020410	Yes		Yes	Yes	Yes								Category 1: 3 years; Category 2 – 12: 2 year
88	RFC2018019275	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
89	RFC2018019277	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 year
90	RFC2018019276		Yes	Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
91	RFC2018019506	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
92	RFC2018019278		Yes	Yes	Yes									Category 2 – 12: 2 year
93	RFC2018019280			Yes	Yes				Yes					Category 2 – 12: 2 year

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
94	RFC2018019279		Yes	Yes	Yes									Category 2 – 12: 2 year
95	RFC2018019507	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
96	SERC2016016494			Yes	Yes					Yes				Category 2 – 12: 2 years
97	SERC2017017853			Yes	Yes					Yes				Category 2 – 12: 2 years
98	WECC2018020145	Yes		Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 years
99	WECC2017017689	Yes		Yes	Yes	Yes			Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 years
100	WECC2016016415	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
101	WECC2018018940	Yes		Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 years
102	WECC2017018481	Yes		Yes	Yes	Yes				Yes				Category 1: 3 years; Category 2 – 12: 2 years
103	WECC2017018585	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
104	WECC2017018586			Yes	Yes					Yes	Yes			Category 2 – 12: 2 years
105	WECC2017018587			Yes	Yes					Yes	Yes			Category 2 – 12: 2 years
106	WECC2017017879	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2018020777	CIP-007-6	R3.3.3.	██████████ ("the Entity")	██████████	04/30/2018	05/03/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On December 6, 2018, the Entity submitted a Self-Report stating that, as a ██████████, it was in noncompliance with CIP-007-6 R3 Part 3.3.</p> <p>This noncompliance started on April 30, 2018, when the Entity updated antivirus signatures on three (3) PACS workstations prior to testing them and ended on May 3, 2018, when the Entity removed the untested antivirus signatures from the three (3) PACS workstations.</p> <p>An analyst discovered that antivirus signatures were being applied to the Physical Access Control System (PACS) without being tested while working on the project to roll out the new antivirus software to replace the old ██████████ solution. The Entity's documented procedure is to test antivirus signatures on non-NERC "corporate" assets for 24 hours before installing the antivirus signatures on NERC related Cyber Assets. Untested antivirus signatures were applied to three PACS Cyber Assets because an analyst had mistakenly installed the wrong antivirus software package on the PACS Cyber Assets. The wrong antivirus signature package remained on the PACS Cyber Assets for a period of four days without having first been tested as required. The correct package would have delayed installing antivirus signatures for 24 hours while the signatures were being tested on non-NERC assets.</p> <p>The Entity performed an extent of condition review of other NERC related Cyber Assets and determined the issue was limited to the three (3) PACS Cyber Assets. The Cyber Assets reviewed included Windows workstations, Windows servers, and Linux servers with antivirus package installed.</p> <p>The cause of this issue is the lack of a desk-level procedure (DLP) to guide the analysts to create and deploy an antivirus package for the NERC related Cyber Assets that are in the corporate environment.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>The risk with untested antivirus signatures is that a faulty antivirus signature might cause the PACS to become unresponsive (or "crash"). A crash might temporarily hinder physical access, but it would not change the status of any BPS Cyber Assets. A crash could also cause antivirus to stop scanning for viruses. However, the Cyber Assets would still have been protected by internal controls such as hardening techniques and the intrusion detection system.</p> <p>The risk was reduced as the PACS do not directly control BPS Facilities, nor interact with Cyber Assets that do.</p> <p>No harm is known to have occurred to the reliability of the BPS because all the antivirus signatures that were installed without testing were subsequently tested without incident and reinstalled on the PACS Cyber Assets.</p> <p>FRCC determined the Entity's compliance history should not serve as a basis for applying a penalty.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) uninstalled the signature/patterns and reconfigured system on PACS workstations; 2) modified the detective control to include on the NERC Dashboard two additional charts: 1) Windows assets with less than 1-day old antivirus signatures; 2) Linux assets with less than 1-day old antivirus signatures. This provides situational awareness for analysts to quickly identify potential issues with the delay mechanism; 3) performed extent of condition review and investigated other NERC devices and determined the issue was limited to the three (3) PACS devices. The devices reviewed include Windows workstation and Windows server and Linux servers with antivirus installed; 4) performed root cause analysis; 5) expanded preventative control of the security controls validation form (CIP-010), specifically for CIP-007-6 R3 validation, to review corporate assets when the antivirus client is installed on a new OS within the NERC environment; 6) created a preventative control with a new DLP to create antivirus packages to NERC and non-NERC Cyber Assets within the corporate environment and communicate procedure; 7) created a preventative control with a new DLP to deploy antivirus packages to NERC and non-NERC Cyber Assets within the corporate environment and communicate procedure; 8) performed preventative control one-time training for service desk and field analysts on new DLP. Created a knowledge article for the department's knowledgebase, which is used for day-to-day support. New employees are trained with the knowledgebase; and 9) performed preventative control one-time training and communicated to other required personnel the new DLP and changes to the security controls validation form (CIP-010) specifically for CIP-007-6 R3. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2018020721	CIP-010-2	R1.1.2.	██████████ ("the Entity")	██████████	04/16/2018	04/17/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On November 20, 2018, the Entity submitted a Self-Report stating that, as a ██████████, it was in noncompliance with CIP-010-2 R1 Part 1.2.</p> <p>This noncompliance started on April 16, 2018, when the Entity failed to authorize a software license key update to one (1) Electronic Access Control and Monitoring System (EACMS) Cyber Asset that modified the software opening a new port which deviated from the existing baseline and ended on April 17, 2018 when the Entity uninstalled the unauthorized change to the software.</p> <p>License key updates are parameter changes that do not normally affect the software thereby changing the baseline configuration. Therefore, this type of change was not managed under the Entity's change management controls.</p> <p>The Entity performed an extent of condition review of license key installations for similar changes. No prior license key installations have ever opened a port and no additional instances were discovered. The Entity also took steps to ensure license key update issue did not affect any other category of its Cyber Assets.</p> <p>The cause for this noncompliance was determine by the Entity to be a failure to anticipate that license key updates can sometimes trigger changes to baseline configurations. The Entity did not have a standard approach to create a change order before installing the license key because the Entity had not experienced an occurrence like this before.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>The risk was the unauthorized software change opening a port could have allowed unauthorized access to the EACMS Cyber Asset potentially impacting the reliability of the BPS.</p> <p>The risk was reduced because the license key update was from a trusted source that was unlikely to introduce an exposure, was loaded on only one (1) device, and was promptly detected and removed within one day.</p> <p>The unauthorized license key update was promptly removed, then was later tested and reinstalled under the Entity's change control process without any adverse effect on the system.</p> <p>FRCC determined the Entity's compliance history should not serve as a basis for applying a penalty. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) uninstalled the change; 2) performed an extent of condition review of other NERC Cyber Assets to ensure config/change processes are followed. Reviewed other area's/group's methodology/processes that deploy software license keys to determine if this documented issue could or did occur; 3) completed root cause analysis; 4) implemented preventative controls creating a procedure to get authorization to change license keys; and 5) implemented preventative controls to provide one-time training for responsible subject matter experts on new procedure for installing license keys. New employees will receive training on the CIP-007 and CIP-010 process along with the annual mandatory NERC training. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2018020697	CIP-010-2	R2.2.1.	██████████ ("the Entity")	██████████	03/15/2018	04/05/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On November 19, 2018, the Entity submitted a Self-Report stating that, as a ██████████, it was in noncompliance with CIP-010-2 R2.</p> <p>This noncompliance started on March 15, 2018, when the Entity failed to monitor baseline configurations for two (2) Electronic Access Control or Monitoring Systems (EACMS) and ended on April 5, 2018 when the Entity performed the baseline configuration monitoring.</p> <p>Manual monitoring for baseline changes was performed 23 days late for two (2) EACMS. The baseline configurations were manually monitored on February 6, 2018 and again on April 5, 2018. The 58 days between these monitoring events is 23 days over the 35-day period allowed under CIP-010-2, R2.</p> <p>The noncompliance was discovered on April 4, 2018 by another Entity employee while he was logging his manual monitoring. The Entity employee noticed that the review for the two (2) EACMS appliances in March was missing. The individual responsible for monitoring the two (2) appliances performed the manual monitoring function on February 6, 2018, then subsequently retired. However, the responsibility to perform the manual monitoring function was not transferred to another analyst. The extent of condition review revealed no additional instances.</p> <p>The cause for this noncompliance was determine by the Entity to be a lack of a formal process to transfer the responsibility when the person assigned to that task retires or transfers.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>Specifically, the Entity's failure to monitor the two (2) appliances for baseline configuration changes could have allowed an unauthorized change to go undetected thereby posing risk of unauthorized access to BES Cyber Assets.</p> <p>The risk was reduced because the issue was discovered and corrected within a relatively short 23-day period, and any exploitation of this delay risk was mitigated by the Entity's layered protections against cyber threats (e.g. firewalls, multi-factor authentication, unique credentials, etc.) that someone would need to circumvent.</p> <p>FRCC determined the Entity's compliance history should not serves as a basis for applying a penalty. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) reviewed and monitored for changes to the baseline for the two (2) appliances; 2) completed extent of condition by reviewing other manually monitored devices to ensure devices were reviewed at least once every 35 days; 3) performed root cause analysis; 4) implemented preventative controls to include appropriate personnel in the distribution lists for a shared mailbox that is a catch all to ensure assignee on deliverables is updated; 5) developed language for formal NERC separation checklist item to be added to the current HR separation checklist; and 6) implemented preventative controls to have HR publish updated HR separation checklist on intranet website. The separation checklist will be a control to ensure NERC responsibilities are transferred. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020297	CIP-007-6	R5	[REDACTED]	[REDACTED]	12/19/2017	3/27/2018	Self-Log	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)</p>			<p>On July 13, 2018, [REDACTED] submitted a self-log stating that as a [REDACTED] it was in noncompliance with CIP-007-6 R5. [REDACTED] is registered in the [REDACTED]. The noncompliance impacted Cyber Assets that were located [REDACTED].</p> <p>[REDACTED] identified two instances of noncompliance with CIP-007-6 R5.</p> <p>In the first instance of noncompliance, [REDACTED] states that a SME performing password changes for multiple accounts lost the ability to gain access and change the password for a single application domain level account that is used to access ten EACMS devices; the ten devices are located in [REDACTED]. The SME was unable to gain access to the account and change the password prior to the 15-month deadline as required by P5.6. The noncompliance was caused by [REDACTED] failure to follow its process for updating an account password. The noncompliance began on December 19, 2017, when the password age exceeded 15 months, and ended on February 27, 2018, when the password was changed.</p> <p>In the second instance of noncompliance, [REDACTED] states that it failed to enforce authentication of interactive user access as required by P5.1. Specifically, a System Operator failed to logoff from a BES Cyber Asset at the end of a shift and the subsequent System Operator initiated interactive user access under the prior System Operator's access; the BES Cyber Asset was located in [REDACTED]. [REDACTED] reports that technical support staff detected the noncompliance during the second System Operator's shift. The cause of the noncompliance was that [REDACTED] failed to execute its methods for enforcing authentication for interactive user access. The noncompliance began on March 27, 2018 when the second System Operator assumed the first System Operator's interactive access to the BES Cyber Asset, and ended later that day when the System Operator logged off and authenticated with their own credentials.</p> <p>The duration of the noncompliance was noncontiguous; the noncompliance began on December 19, 2017, when the account's password age exceeded 15 months, and ended on March 27, 2018, when the System Operator logged off and authenticated with their own credentials.</p>					
<p>Risk Assessment</p>			<p>The noncompliance poses a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance of noncompliance was minimal because [REDACTED] had taken steps to reduce the exposure of the account and password. Per [REDACTED] the credentials for the account were secured in a Password Management tool; the tool logs all users who view the password, and [REDACTED] had taken steps to limit the tool's number of users. Additionally, [REDACTED] reports that it conducted an extent of conditions analysis and determined that the noncompliance did not impact any other passwords. Moreover, per [REDACTED] there was no unauthorized access to the account during the period of noncompliance. Finally, [REDACTED] states that the noncompliance did not impact any BES Cyber Asset. No harm is known to have occurred.</p> <p>The second instance of noncompliance was also minimal. Per [REDACTED] the noncompliance did not have the potential for unauthorized access, as both System Operators had the same permission level on the BES Cyber Asset. Additionally, [REDACTED] technical system for enforcing authentication for interactive user access was operating correctly, and the noncompliance was limited to the failure of a System Operator to follow the manual shift change process. Moreover, the noncompliance did not compromise the credentials of either System Operator. Finally, both System Operators have current CIP Training, Personnel Risk Assessments, and are certified System Operators. No harm is known to have occurred.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, [REDACTED]</p> <p>To mitigate the first instance of noncompliance [REDACTED]</p> <ol style="list-style-type: none"> 1) changed the password on the account; 2) ensured that the SME had appropriate access to be able to change the password; 3) conducted an extent of condition analysis to determine if there were any additional expired passwords; and 4) implemented a new report that will be generated weekly, which will list all passwords aged over 12 months, and the report will be reviewed as part of its cyber security operational practices. <p>To mitigate the second instance of noncompliance [REDACTED]</p> <ol style="list-style-type: none"> 1) logged out of the BES Cyber Asset and authenticated with their own credentials; 2) reinforced the issue during System Operator training; and 3) augmented the wording in its System Operator shift turnover procedure to emphasize the need to logoff and logon. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020300	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/1/2016	6/12/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 13, 2018, [REDACTED] submitted a self-log stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R1. [REDACTED]. The noncompliance impacted a Cyber Asset that was located in [REDACTED].</p> <p>[REDACTED] states that during its Vulnerability Assessment it discovered that it had incorrectly documented the firmware version for a PCA located at a substation as required by P1.1.1. [REDACTED] reports that for this PCA, it could not utilize its baselining tool and had to manually collect and document its baseline attributes. [REDACTED] reports that it accidentally documented the incorrect firmware version in the baseline documentation. The documentation error affected the device's password complexity, as the documented firmware version could not support the complexity requirements of CIP-007-6 P5.5, but the actual firmware version could support those requirements.</p> <p>The cause of the noncompliance was that [REDACTED] failed to implement its manual process for documenting baselines.</p> <p>The noncompliance began on July 1, 2016 when the Standard became enforceable, and ended on June 12, 2018 when the baseline was updated.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The scope of the noncompliance was limited to a single PCA; [REDACTED] stated that it conducted an extent of condition analysis of the same and similar model Cyber Assets and concluded that no other Cyber Assets were similarly noncompliant. Additionally, per [REDACTED] the PCA was serially connected to one BES Cyber Asset and was not accessible via External Routable Connectivity (ERC), limiting the attack vectors to the device; physical access to the PCA was limited as it was in a functioning PSP. Finally, the noncompliance did not affect any applicable security patches, as [REDACTED] states that it confirmed there were no applicable security updates released for the actual version of the firmware during the period of noncompliance. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) updated the baseline of the PCA; 2) changed the password of the PCA; 3) conducted an extent of condition analysis of the same model Cyber Assets; and 4) had its CIP Senior Manager conduct training with applicable SMEs to convey lessons learned, reinforce the importance of accurately documented baselines, discuss human performance factors related to manually documenting baseline attributes, and how to fix conditions related to baselines. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017018654	CIP-006-6	R1	[REDACTED]	[REDACTED]	[REDACTED]	11/13/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On November 14, 2017, [REDACTED] submitted a Self-Report to MRO stating that, as a [REDACTED] it was in noncompliance with CIP-006-6 R1. [REDACTED]. The noncompliance impacted [REDACTED] Control Center [REDACTED].</p> <p>In [REDACTED], [REDACTED] moved its North American Headquarters (including its Control Center) to a new location. [REDACTED] contracted with a physical security vendor to set up and configure its Physical Security Perimeter (PSP) and its Physical Access Control System (PACS) Server Room. During an internal compliance review that occurred in June 2017, [REDACTED] determined that its physical security system was not correctly set up to issue alarms or alerts for unauthorized access to its PSP (P1.5) or its PACS Server Room (P1.7).</p> <p>The cause of the noncompliance was that [REDACTED] failed to select a vendor that could implement the PACS system in a manner that is consistent with the [REDACTED] policy.</p> <p>The noncompliance began on [REDACTED] when [REDACTED] relocated its Control Center and ended on November 13, 2017, when [REDACTED] replaced its PACS system at its Control Center and verified that it was producing the required alert or alarm.</p>					
Risk Assessment			<p>The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The PSP and Server Room had multiple levels of physical security. During the noncompliance, [REDACTED] states that it was still controlling access to the PSP and PACS Server Room. Additionally, [REDACTED] states that it was using 24-hour CCTV to monitor the perimeter of its Headquarters and its Control Center. Finally, there is a 'panic button' in the PSP that automatically contacts local police and first responders. No harm is known to have occurred.</p> <p>[REDACTED] has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) selected a new vendor to replace the physical security system; and 2) verified that the physical security system transmits the alarms or alerts required by P1.5 and P1.7. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019027	CIP-007-6	R4			3/21/2017	8/17/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 11, 2017, [REDACTED] submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-007-6 R4. [REDACTED] stated that the centralized security monitoring and alerting system was not generating alerts for event logging for 24 medium impact BES Cyber Assets at two medium impact substations. [REDACTED] reported that a source code change management error resulted in the corruption of the system's environment variables in the production environment, which stopped the security event alerting. [REDACTED] reported that it conducted an extent-of-conditions review and determined that no other high or medium impact BES Cyber Systems were impacted by the noncompliance.</p> <p>The cause of the noncompliance was that [REDACTED] software development deployment process was flawed and allowed improper changes to be deployed to production.</p> <p>The noncompliance began on March 21, 2017, when the system stopped generating alerts at two substations, and ended on August 17, 2017, when the system was corrected.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was limited to two substations that were on the same Transmission Line. Additionally, the impacted system was an [REDACTED]. Finally, [REDACTED] reports that it manually reviewed logs and determined there were no malicious security events during the noncompliance. No harm is known to have occurred.</p> <p>[REDACTED] relevant CIP-007-6 R4 compliance history includes a prior minimal risk violation of CIP-007-1 R4 ([REDACTED]) that was mitigated on [REDACTED]. MRO determined that [REDACTED] compliance history should not serve as a basis for applying a penalty. The prior noncompliance was distinct as it involved documentation regarding anti-virus signatures, and the current noncompliance and prior noncompliance are separated by a substantial duration of time.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) corrected the configuration of the centralized security monitoring and alerting system; 2) created a predefined functional testing process and checklist to use when performing changes, upgrades, and patches to ensure the system is functioning properly and development configurations are not transferred to production; and 3) created a weekly event count that can be reviewed by security analysts to ensure that security events are being logged and detected. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019028	CIP-007-6	R3			4/18/2017	8/18/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 11, 2017, [REDACTED] submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-007-6 R3. [REDACTED] stated that its threat detection system was unable to detect malicious code for 24 BES Cyber Assets at two medium impact substations. [REDACTED] reported that the system failed after a patch and upgrade was applied to the system. [REDACTED] states that the noncompliance was discovered when a security engineer was investigating another issue related to its centralized security monitoring and alerting system.</p> <p>The cause of the noncompliance was a lack of controls to monitor the functionality of the threat detection system.</p> <p>The noncompliance began on April 18, 2017, when the threat detection system stopped working at two substations, and ended on August 18, 2017, when the threat detection system became operational again.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was limited to two substations that were on the same Transmission Line. Additionally, [REDACTED] stated that the impacted Cyber Assets were protected by a functioning Electronic Security Perimeter (ESP) at all times. Further, the impacted system [REDACTED]. Finally, [REDACTED] reports that it manually reviewed logs and determined there were no malicious security events during the noncompliance. No harm is known to have occurred.</p> <p>[REDACTED] has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) restored the functionality of the threat detection system; 2) created a weekly event count that can be reviewed by security analysts to ensure that security events are being logged and detected; and 3) created a checklist to use when performing upgrades and patches to ensure the system is functioning properly after the upgrade or patch is applied. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020291	CIP-006-6	R2	[REDACTED]	[REDACTED]	11/20/2017	11/20/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On August 7, 2018, [REDACTED] submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-006-6 R2. [REDACTED] stated that an employee left a custodial contractor unescorted for eight minutes in the Physical Security Perimeter (PSP).</p> <p>The cause of the noncompliance was that the employee failed to follow [REDACTED] escort policies.</p> <p>The noncompliance began on November 20, 2017, when the employee stopped escorting the contractor, and ended approximately eight minutes later when the contractor exited the PSP.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] stated that the contractor was confined to a PSP that only had EMS support workstations and the contractor did not have electronic access. Additionally, [REDACTED] reported that the contractor documented the entry and exit on the visitor log. Finally, [REDACTED] stated that the duration was limited to eight minutes. No harm is known to have occurred.</p> <p>[REDACTED] CIP-006-6 R2's relevant compliance history includes a prior minimal risk violation of CIP-006-1 R1 [REDACTED] that was mitigated on December 7, 2012. MRO determined that [REDACTED] compliance history should not serve as a basis for applying a penalty. The prior noncompliance did not involve any escort issues and the current and prior noncompliance are separated by a substantial duration of time.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) had the contractor leave the PSP; and 2) reinforced the escort policy with the employee that left the contractor unescorted. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2017018346	CIP-010-2	R4	[REDACTED]	[REDACTED]	7/19/2017	7/19/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On August 18, 2017, [REDACTED] submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-010-2 R4. [REDACTED] stated that a protection and controls technician connected a corporate laptop to the RTU to change its configuration. [REDACTED] reports that afterwards, the technician realized that he should have used the designated CIP laptop (as required by Transient Cyber Asset policy). [REDACTED] states that the technician reported the incident to the substation compliance engineer.</p> <p>The cause of the noncompliance was that [REDACTED] failed to follow its Transient Cyber Asset policy.</p> <p>The noncompliance began on July 19, 2017, when the technician connected the corporate laptop to the RTU and ended later on July 19, 2017, when the technician disconnected the laptop.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] stated that the corporate laptop was installed with anti-virus, and real time alerts were monitored by the cyber security department; the laptop showed no presence of malicious code. Further, [REDACTED] reported that there were no baseline changes to the RTU. Finally, the noncompliance was limited to one substation as there was no External Routable Connectivity to that substation. No harm is known to have occurred.</p> <p>[REDACTED] has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) checked for any baseline changes to the RTU; 2) modified the ticketing system to automatically insert "USE CIP LAPTOP AT THIS SUBSTATION" when any work order for a modification is created for a medium impact substation; and 3) added additional signage to medium impact substation connection points to improve the awareness to use the CIP laptop. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020294	CIP-007-6	R2	[REDACTED]	[REDACTED]	3/3/2018	3/21/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 10, 2018, [REDACTED] submitted a self-log stating that, as a [REDACTED] it was in noncompliance with CIP-007-6 R2. Specifically, [REDACTED] stated that it failed to apply an applicable patch (or create a dated mitigation plan) within the time frame required by P2.3. The noncompliance involved a single patch that was not applied to three PACS devices. [REDACTED] states that it utilizes work orders assigned to SMEs to track the application of patches. [REDACTED] stated that it discovered the noncompliance when a SME was reviewing his open work orders and discovered that the associated change request ticket had been drafted but not submitted.</p> <p>The cause of the noncompliance is that [REDACTED] failed to execute its process for implementing security patches.</p> <p>The noncompliance began on March 3, 2018, 36 days after the patch was evaluated, and ended on March 21, 2018, when the patch was applied.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The PACS devices are protected [REDACTED], which limited the external exposure of the servers. Additionally, the scope of the noncompliance was limited to one patch on three PACS devices. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) the patch was applied to the PACS devices; and 2) modified the change management software's dashboard to display a count of open work orders the user currently has. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019105	CIP-011-2	R1	[REDACTED]	[REDACTED]	5/2/2017	9/12/2017	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On January 12, 2018, [REDACTED] submitted a self-log, stating that as a [REDACTED] it was in noncompliance with CIP-011-2 R1. Specifically [REDACTED] stated that it did not implement its procedure(s) for protecting BES Cyber System Information (BES CSI) when two work orders had an attachment that contained BES CSI regarding high impact BES Cyber Assets and medium impact BES Cyber Assets. Those work order attachments were available to employees in the Information Technology (IT) department that were not authorized to view that BES CSI.</p> <p>The cause of the noncompliance was that [REDACTED] failed to follow its written procedures for work orders associated with BES CSI.</p> <p>The noncompliance began on May 2, 2017, when the BES CSI was attached to two work orders, and ended on September 12, 2017, when the work orders were revised.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] stated that the attached BES CSI did not provide information that could provide control or interactive user access to the BES Cyber Assets (e.g. log-in information or IP addresses). Per [REDACTED] the work orders were saved to a location that met its BES CSI storage procedures. Finally, the noncompliance was limited to exposure to IT employees who have been trusted with similarly critical information technology information. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) revised the work orders; and 2) reviewed and reinforced written BES CSI procedures with applicable IT staff. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019580	CIP-004-6	R5	[REDACTED]	[REDACTED]	9/24/2016	2/16/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 10, 2018, [REDACTED] submitted a self-log stating that as a [REDACTED], it was in noncompliance with CIP-004-6 R5. Specifically, [REDACTED] identified three instances where it did not revoke an individual's logical access to its EMS application as required by P5.2 and P5.4. [REDACTED] stated that all of these instances involved removing logical access to the EMS application. Per [REDACTED] the process for revoking an employee from the EMS application requires sending a manual reminder email to the employee responsible for maintaining the EMS operators table; in these three instances [REDACTED] stated that the responsible employee did not receive that email request.</p> <p>The first instance of noncompliance involved an employee who was transferred to a new position on September 22, 2016. [REDACTED] did not revoke the individual's EMS application account by the end of the next calendar day as required by P5.2. [REDACTED] stated that it discovered the employee still had logical access to the EMS application on May 8, 2017 and removed that account the same day. The individual was later transferred back to the EMS group and was re-authorized for the same access.</p> <p>The second instance of noncompliance involved an employee who was terminated (not for cause). [REDACTED] revoked the individual's ability for Interactive Remote Access within 24 hours as required by P5.1, but did not revoke the individual's EMS application account (a non-shared user account) within 30 days as required by P5.4. [REDACTED] stated that the noncompliance began on January 28, 2018, and that it discovered the employee still had an EMS application account on February 16, 2018 and removed that account the same day.</p> <p>The third instance of noncompliance involved an employee who was terminated (not for cause) on February 5, 2018. [REDACTED] revoked the individual's ability for Interactive Remote Access within 24 hours as required by P5.1, but did not revoke the individual's EMS application account (a non-shared user account) within 30 days as required by P5.4. [REDACTED] stated that the noncompliance began on February 5, 2018, that it discovered the employee still had an EMS application account on February 16, 2018 and removed that account the same day.</p> <p>[REDACTED]</p> <p>The cause of the noncompliance is that [REDACTED] relied upon a manual process to remove an individual from the EMS application.</p> <p>The noncompliance was noncontiguous. The noncompliance began on September 24, 2016, when the individual's access to the EMS application was not revoked by the end of the next calendar day after transfer in the first instance of noncompliance, and ended on February 16, 2018, when the individuals' non-shared user account was revoked in the second and third instance of noncompliance.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the bulk power system. Per [REDACTED] the individuals should not have been able to gain unauthorized access, as [REDACTED]. Additionally, [REDACTED] stated that the individual in instance one remained employed by [REDACTED] during the period of noncompliance (eventually transferring back to a role that required this same level of access) and that the individuals in instance two and instance three resigned from [REDACTED] not for cause. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) deleted the user accounts from the EMS application; and 2) created an automatic notification to be sent to the employee responsible for maintaining the EMS operators' table anytime there is a change in the relevant Active Directory groups. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017016749	CIP-004-6	R2	[REDACTED]	[REDACTED]	7/1/2016	1/11/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On January 5, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R2. Specifically, during a review of its SCADA vendor's training materials, it discovered that the vendor's training materials provided to its employees did not include all the components required by the subparts of the Standard. Specifically, the vendor's training content did not include: [REDACTED] cyber security policies (P2.1.1); [REDACTED] visitor control program (P2.1.4); plans for how to identify, respond, or recover from a Cyber Security Incident (P2.1.6-P2.1.8); and content on the cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets and Removable Media (P2.1.9).</p> <p>The noncompliance was caused by a lack of rigor in [REDACTED] processes that resulted in a failure to verify that the training created and provided by the vendor met [REDACTED] requirements.</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became enforceable and ended on January 11, 2017, when the SCADA vendor's were retrained with materials that included all the subparts.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The vendor's employees received training that covered multiple subparts of the Standard. Further, the vendor's employees only had access to medium impact BES Cyber Systems as the Control Center only controls low impact BES Cyber Assets. No harm is known to have occurred.</p> <p>[REDACTED] has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) ensured that the impacted individuals received training which incorporated the six sub-requirements missed in the previous training program; 2) published a new program for contractors and vendors whose staff require CIP training; the program requires the contractor/vendor perform training with materials provided by [REDACTED] the trainees must pass a completion test, and the contractor/vendor supply the passed tests to [REDACTED] and 3) emailed the impacted contractor regarding the changes to the program and listed the requirements needed to correct the issue. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2017017624	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/1/2016	7/1/2017	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 5, 2017, [REDACTED] submitted a self-log stating that as a [REDACTED] it was in noncompliance with CIP-010-2 R1. [REDACTED] later submitted an updated self-log on May 22, 2017.</p> <p>[REDACTED] stated that it did not include UDP ports in the baseline for its medium-impact BES Cyber Systems. The responsible SME(s) did not believe that the Standard and Requirement required the documentation of UDP ports and only scanned for open TCP ports, resulting in only TCP ports being included in the baselines.</p> <p>The cause of the noncompliance was that [REDACTED] processes lacked sufficient detail to ensure that UDP ports were included in baselines.</p> <p>The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable and ended on July 1, 2017, when system scans were complete and the baselines had been updated to include the UDP baselines.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was minimal because per [REDACTED] the scope of the noncompliance was limited to two UDP ports, both ports were necessary (thus the noncompliance was limited to proper documentation), and the firewall rules prevented remote access to and from the two UDP ports. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) performed UDP scans of its systems and updated the required baselines; 2) updated associated documentation to explicitly state UDP and TCP ports; 3) provided informal training to applicable SMEs about the importance of both UDP and TCP ports; and 4) added each Cyber Asset into a compliance monitoring tool that maintains a list of all enabled listening ports that specifically calls out UDP and TCP ports. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020629	CIP-010-2	R1	[REDACTED]	[REDACTED]	11/22/2016	4/11/2017	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 5, 2017, [REDACTED] submitted a self-log stating that as a [REDACTED] it was in noncompliance with CIP-010-2 R1. [REDACTED] later submitted an updated self-log on May 22, 2017. [REDACTED] identified three instances of noncompliance in its self-log.</p> <p>In the first instance of noncompliance, [REDACTED] made a baseline change to an EACMS associated with a medium impact BES Cyber System prior to requesting authorization. [REDACTED] stated that the engineer applied the change and then requested authorization, which was granted later that day. The cause of the noncompliance was that the engineer failed to follow the process for requesting authorization. The noncompliance began on November 22, 2016, and ended later that day.</p> <p>In the second instance of noncompliance, [REDACTED] made an approved change to multiple network switches, but failed to update the baseline within 30 days. [REDACTED] stated that the cause of the noncompliance was that the engineer responsible for the baseline change failed to follow the documented process, and acknowledged a task reminder without performing the task. The noncompliance began on February 9, 2017, 31 days after the change was applied, and ended on February 14, 2017, when the baseline change was documented.</p> <p>In the third instance of noncompliance, [REDACTED] replaced an EACMS device with a spare of the same model. [REDACTED] stated that the spare EACMS had an updated firmware version, which, when put into production, did not match the documented baseline. [REDACTED] reports its asset management tool detected the change during a routine scan. [REDACTED] states that it failed to follow its process for a device replacement. The noncompliance began on March 31, 2017 when the spare was put into production, and ended on April 11, 2017, when the spare's firmware was rolled back to conform with the baseline.</p> <p>The noncompliance was noncontiguous; it began on November 22, 2016, when the engineer applied the change in the first instance, and ended on April 11, 2017, when [REDACTED] rolled back the spare's firmware in the third instance.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance of noncompliance was minimal because, per [REDACTED] the patch did not change any cyber security controls on the device, the scope of the noncompliance was limited to one EACMS device, and the duration of the noncompliance was limited to less than one day. No harm is known to have occurred.</p> <p>The second instance of noncompliance was minimal because, per [REDACTED] the noncompliance was limited to a documentation issue and the duration of the noncompliance was limited to six days. No harm is known to have occurred.</p> <p>The third instance of noncompliance was minimal because, per [REDACTED] the firmware version in the spare had been used previously in non-production testing, the scope of the noncompliance was limited to one device, and the duration of the noncompliance was limited to eleven days. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <p>To mitigate instance one, [REDACTED] 1) submitted and approved a change request; and 2) verified that the procedure was clear and then provided reinforcement training to the engineer.</p> <p>To mitigate instance two, [REDACTED] 1) updated the baseline; 2) provided additional training to the engineer; and 3) implemented automatic workflows to require completion of associated processes before closing the workflow.</p> <p>To mitigate instance three, [REDACTED] 1) rolled back the firmware version on the spare; and 2) now requires a change request be created for all Cyber Assets being put into or removed from service as an additional oversight control for the replacement process.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019574	CIP-007-6	R2	[REDACTED]	[REDACTED]	2/15/2018	3/7/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 6, 2018, [REDACTED] submitted a self-log stating that as a [REDACTED] it was in noncompliance with CIP-007-6 R2. [REDACTED] stated that it failed to evaluate four security patches within 35 days of the previous evaluation period as required by P2.2. The four security patches impacted 13 Cyber Assets associated with medium impact BES Cyber Systems in the substation environment. [REDACTED] reports that a configuration change to its system caused the patches to not be evaluated. [REDACTED] reports that the noncompliance was discovered by a SME who was performing a secondary evaluation of the patch source. [REDACTED] reports that upon detection, the patches were promptly evaluated and placed on a mitigation plan that same day.</p> <p>The cause of the noncompliance was that [REDACTED] security patch evaluation process for offline patching lacked sufficient detail regarding change verification, resulting in the security patches not being evaluated within 35 days.</p> <p>The noncompliance began on February 15, 2018, 36 days after the last patch evaluation and ended later on March 7, 2018, when the patches were evaluated and placed on an existing mitigation plan.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] states that the patches were added to an existing mitigation plan 56 days after the last patch evaluation, which is less than the 70 days allowed by P2.2 and P2.3. Additionally, per [REDACTED] the impacted Cyber Assets did not have any External Routable Connectivity (ERC) and were afforded additional protections above the minimum requirements including unused physical port blockers, a dedicated USB device to connect to the Cyber Assets, and a hardened Transient Cyber Asset used to connect to the Cyber Assets. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) evaluated the patches and applied them to a mitigation plan; and 2) added an additional step to the process that directs the evaluator to perform a second verification step with the vendor's website if no security patches are evaluated. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020143	CIP-010-2	R1			1/17/2018	4/12/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 10, 2018, [REDACTED] submitted a self-log stating that, as a [REDACTED] it was in noncompliance with CIP-010-2 R1. Specifically, [REDACTED] did not authorize a change to two PACS devices as required by P1.2 and did not update the baseline configuration within 30 days as required by P1.3. [REDACTED] stated that it was installing a new firewall and had authorized that change, but the authorized change documentation did not include the required installation of the firewall software on the PACS servers. As a result, the software installation was not authorized for the PACS devices and the baseline of the PACS devices was not updated within 30 days of the change. [REDACTED] states that it discovered the noncompliance during a scan performed by its asset management tool. [REDACTED] conducted an extent of conditions to determine if the software was installed on any other Cyber Assets.</p> <p>The cause of the noncompliance was that [REDACTED] process for identifying additional systems or devices impacted when performing changes lacked sufficient detail.</p> <p>The noncompliance began on January 17, 2018, when the software was installed, and ended on April 12, 2018, when the change was authorized and the baseline was updated.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] stated that the scope of the noncompliance was limited two PACS devices. Further, [REDACTED] reports that the PACS devices were located in a [REDACTED], which exceeds the requirements of the Standard. Finally, the installation of the software did not open any additional network ports and there were no security patches released for the software during the period of noncompliance. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) authorized the software change and updated the baselines; 2) improved the process that applies to firewalls by updating its firewall change management process to require the review of the firewall software management tool to identify any Cyber Assets that the firewall software was installed on; and 3) augmented its compliance management software to issue a notification (prior to the 30-day timeframe) when a Cyber Asset's baseline has a difference that has not been addressed. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018018951	CIP-007-6	R2	[REDACTED]	[REDACTED]	8/6/2016	7/26/2017	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 16, 2017, [REDACTED] submitted a self-log to MRO stating that, as a [REDACTED] (hereafter referred to as [REDACTED]), it was in noncompliance with CIP-007-6 R2. [REDACTED] The noncompliance occurred in [REDACTED]. In the self-log, [REDACTED] identified three instances of potential noncompliance, however, MRO determined that only two of the instances constituted noncompliance.</p> <p>In the first instance of noncompliance, [REDACTED] stated that it identified two patches that were evaluated outside of the 35-day requirement (P2.2). [REDACTED] reported that the two patches were released on [REDACTED] but were not evaluated until January 24, 2017. [REDACTED] states that it applied the patches on February 22, 2017. [REDACTED] states that the patches applied to devices that are used to monitor and control access (EACMS) to substation Electric Security Perimeters (ESPs) and devices that monitor and controls access (PACS) to Physical Security Perimeters (PSPs). Per [REDACTED] the devices monitor and control access to PSPs and substation ESPs in the [REDACTED] system. The cause of the noncompliance was that [REDACTED] did not implement its documented Patch Management. The noncompliance began on [REDACTED] 36 days after the patch was released, and ended on January 24, 2017, when the patch was evaluated.</p> <p>In the second instance of potential noncompliance, [REDACTED] stated that prior to July 1, 2016, it identified a security patch that was not applied to all applicable devices. [REDACTED] reports that a patch was released that applied to three models of a device, but only needed to be applied if the devices were Ethernet-connected. As a result, [REDACTED] distributed work packets to relay technicians that only instructed them to apply the patch to the Ethernet-connected devices. As a part of CIP V5, 29 of these devices became Ethernet-connected later, and the patch was not applied to those 29 devices as required by P2.3. The 29 devices were located at substations in the [REDACTED] and [REDACTED] system. [REDACTED] states that after discovery of this noncompliance, it created a mitigation plan on July 26, 2017, and installed the patches by July 31, 2017. The cause of the noncompliance was a policy that applied patches based on device connectivity rather than device capability. The noncompliance began on August 6, 2016, 36 days after the Standard and Requirement became enforceable and ended on July 26, 2017, when [REDACTED] created a mitigation plan to apply the patch.</p> <p>The noncompliance began on August 6, 2016, 36 days after the Standard and Requirement became enforceable and ended on July 26, 2017, when [REDACTED] created a mitigation plan to apply the patch in the third instance of noncompliance.</p>					
Risk Assessment			<p>The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>For the first instance of noncompliance, [REDACTED]. Additionally, [REDACTED] stated that the affected devices are isolated from any Internet connection, [REDACTED]. No harm is known to have occurred.</p> <p>For the second instance of noncompliance, per [REDACTED] the potential harm from the patched vulnerability was limited to denying remote access to the relays and the vulnerability did not provide a pathway that could have tripped the relays or altered relay settings. Further, the relays were located within functioning PSPs and ESPs (whose Electronic Access Points are designed to deny access by default). [REDACTED]. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the first instance of potential noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) evaluated and applied the patches; and 2) implemented a monthly patch management coordination meeting. <p>To mitigate the second instance of potential noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) placed the relays on a mitigation plan and applied the patches; 2) provided refresher training to field personnel; and 3) changed its process to install patches based upon device capability rather device connectivity. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020135	CIP-004-3a	R2	[REDACTED]	[REDACTED]	8/27/2015	9/29/2017	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 10, 2018, [REDACTED] submitted a self-log stating that, as a [REDACTED], it was in noncompliance with CIP-004-3a R2. During its periodic review of individuals with unescorted physical access, [REDACTED] determined that an employee no longer needed that access. [REDACTED] stated that during the removal process, it discovered that the employee was not in the tracking system used to track CIP training. [REDACTED] stated that it had no record that the employee had been trained after August 26, 2014.</p> <p>The cause of the noncompliance was that in preparation of the CIP v5 transition, [REDACTED] implementation of its new training tracking system lacked rigor, resulting in one employee not being inputted into the new training tracking system.</p> <p>The noncompliance began on August 27, 2015, one year and one day after the employee's last documented training, and ended on September 29, 2017 when the employee's physical access was removed.</p>					
Risk Assessment			<p>The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] stated that the employee only had physical access and did not have electronic access. Additionally, [REDACTED] reported that the noncompliance was limited to a failure to provide refresher training as opposed to a failure to provide any training, that the employee remained employed at all times during the noncompliance, and the employee had an up to date personnel risk assessment (PRA). Further, per [REDACTED] the employee had access to Cyber Security awareness materials that were generally available to all employees that could assist the employee respond to or identify an event. Finally, [REDACTED] states that the noncompliance was limited in scope to the failure to bring one employee into a new database for CIP v5 transition. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) removed the physical access from the employee; and 2) created a new workflow to confirm that the required training has been completed before granting access. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020148	CIP-006-6	R1	[REDACTED]	[REDACTED]	2/15/2018	2/15/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 10, 2018, [REDACTED] submitted a self-log to MRO stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R1. On February 15, 2018, [REDACTED] performed maintenance on a physical access control system (PACS) panel that controlled access to the Control Center. [REDACTED] stated that after the maintenance, it failed to manually re-enable the [REDACTED].</p> <p>The cause of the noncompliance was that [REDACTED] failed to follow its process to manually re-enable [REDACTED] following maintenance activities.</p> <p>The noncompliance began on February 15, 2018, when [REDACTED] failed to re-enable [REDACTED] after maintenance and ended two hours and sixteen minutes later when [REDACTED] manually re-enabled [REDACTED].</p>					
Risk Assessment			<p>The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED]. Additionally, the Control Center is nested within a corporate security perimeter, which limited the potential for unauthorized access. Further, the noncompliance occurred during normal work hours, meaning that company personnel were within the vicinity of the door reducing the risk from an unauthorized access. Finally, [REDACTED] reviewed access logs from the period of noncompliance and determined there were no unauthorized access attempts. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) [REDACTED]; 2) worked with its vendor to implement a solution where [REDACTED]; and 3) sent a reminder to applicable staff to manually re-enable [REDACTED] every time a PACS panel is reallocated or power-cycled. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019023	CIP-004-6	R4	██████████	██████████	7/1/2016	8/2/2017	Self-Report	2/28/2019 Expected Date
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On January 8, 2018, ██████ submitted a Self-Report stating that as a ██████ it was in noncompliance with CIP-004-6 R4. Specifically in August 2017, during a periodic review, ██████ stated that it discovered an employee that had unauthorized physical access to its Back-Up Control Center (BUCC). The employee was responsible for facilities maintenance for all of ██████ buildings, including its substations, ██████. ██████ stated that the employee's access badge did not provide access to the Primary Control Center. ██████ states that the individual was employed prior to July 1, 2016, and that it is unclear when the employee was granted access to the BUCC.</p> <p>The cause of the noncompliance was that ██████ failed to apply its processes to authorize unescorted physical access. Additionally, the cause of the long duration of the noncompliance is that RPU's processes related to its quarterly review were lacking.</p> <p>The noncompliance began on July 1, 2016 when the Standard and Requirement became enforceable, and ended on August 2, 2017.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. ██████ stated that the unauthorized access was limited to the BUCC and that the employee did not have access to the Primary Control Center. Additionally, ██████ reports that the individual did not have electronic access to BES Cyber Systems. Further, ██████ reports that the employee only accessed the BUCC once during the period of noncompliance. Finally, the employee was subsequently authorized for unescorted physical access to the BUCC. No harm is known to have occurred.</p> <p>██████ has taken steps to prevent reoccurrence during the mitigating activities completion period by enhancing its quarterly review process and adding internal controls to its PACS software.</p> <p>██████ has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, ██████</p> <ol style="list-style-type: none"> 1) revoked the employee's physical access; 2) updated its quarterly review process to include a system generated report to provide enhanced controls; and 3) enabled logging on its PACS software to provide better change control on its access lists. <p>To mitigate this noncompliance, ██████ will complete the following mitigation activities by February 28, 2019:</p> <ol style="list-style-type: none"> 1) replace the paper authorization process with an electronic access form in its documentation management system; and 2) provide additional training for all employees involved in the access and revocation process. <p>The length of time to complete the remaining mitigating activities is the result of ██████ investigating different solutions and securing funding for the solution in the 2019 budget.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2018019304	CIP-002-5.1a	R2	[REDACTED]	[REDACTED]	10/1/2017	12/21/2017	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 28, 2018, [REDACTED] submitted a Self-Certification stating [REDACTED] it was in noncompliance with CIP-002-5.1a R2. [REDACTED] stated that on October 1, 2017, it conducted its annual review of its Control Centers as required by P2.1. [REDACTED] reports that four network switches were initially classified as EACMS, but became BES Cyber Assets due to modifying the functions prior to the annual review. [REDACTED] states that it did not recognize the change in functionality during its annual review and thus did not update the classification as required by P2.1.</p> <p>The cause of the noncompliance was that [REDACTED] process for its annual review was deficient, as it did not include a review of device functionality descriptions.</p> <p>The noncompliance began on October 1, 2017, when the classification of the switches was not updated, and ended on December 21, 2017, when the switches were re-categorized as BES Cyber Assets.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was minimal because per [REDACTED] [REDACTED]. No harm is known to have occurred.</p> <p>[REDACTED] has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) corrected the categorization of the four switches, changing them from EACMS to BES Cyber Assets; and 2) an information verification step was added to the assessment process, which requires that System and Network Administrators must verify accuracy of the asset information prior to the review. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2018019320	CIP-003-6	R1	[REDACTED]	[REDACTED]	7/1/2017	2/21/2018	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 28, 2018, [REDACTED] submitted a Self-Certification stating [REDACTED] it was in noncompliance with CIP-003-6 R1. Specifically, [REDACTED] failed to obtain the signature of its CIP Senior Manager on the review of its physical security cyber security policies as required by P1.1.3 and P1.2.2. As part of a reorganization, [REDACTED] had moved the CIP Senior Manager to a new department and assigned the Security Officer to be responsible for physical security and the physical security plans. Regardless of the reorganization and assignment, under [REDACTED] process the Security Officer is to perform the review and the CIP Senior Manager must approve the review. [REDACTED] reports that after the review conducted, when the Security Officer was signing the document, the additional signature line for the CIP Senior Manager was deleted. [REDACTED] states that the Security Officer then failed to route the documentation to the CIP Senior Manager's for approval.</p> <p>The noncompliance was caused by [REDACTED] failure to follow its process.</p> <p>The noncompliance began on July 1, 2017, 15 months after P1.2 became enforceable, and ended on February 21, 2018, when the CIP Senior Manager approved and signed the review.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance can be accurately regarded as the failure to fully approve a review as opposed to the failure to conduct a review. Additionally, the staff that were involved in the review reported to the CIP Senior Manager. Finally, the version of the plan that was not signed by the CIP Senior Manager only contained one change from the previous signed version. No harm is known to have occurred.</p> <p>[REDACTED] has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) the CIP Senior Manager signed both CIP-003-6 policies; 2) reviewed all documents under the jurisdiction of the Security Officer and verified no other documents had been impacted; 3) assigned the managing of the CIP-003-6 R1 review schedule to the [REDACTED] who will ensure the CIP Senior Manager approves and signs; and 4) created a database for reviews and signatures capable of date tracking and alerting to the requirements of CIP-003-6 R1. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017016900	CIP-007-6	R2			11/22/2016	11/22/2016	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 1, 2017, [REDACTED] submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-007-6 R2. Specifically, [REDACTED] failed to apply an applicable patch within 35 calendar days (or create a dated mitigation plan) as required by P2.3. [REDACTED] states that it evaluated the patch on October 17, 2016 and it should have been applied on or before November 21, 2016; [REDACTED] reports the patch was applied on November 22, 2016. [REDACTED] states that the patch was applicable to four PACS servers.</p> <p>The cause of the noncompliance was that [REDACTED] processes lacked detail to ensure timely action was taken by applicable staff.</p> <p>The noncompliance began on November 22, 2016, 36 days after the patch was evaluated, and ended later that day when the patch was applied.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. [REDACTED] reports that the noncompliance was limited in scope to one patch that applied to four PACS servers. Additionally, [REDACTED] states that the noncompliance was limited to less than one day. No harm is known to have occurred.</p> <p>[REDACTED] has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) applied the patch; 2) implemented a new process where patch evaluations are always performed during the fourth week of the month and patch installations are always performed during the first week of the month, resulting in a 19 day maximum between patch evaluation and patch installation; and 3) implemented calendar reminders to evaluate patches, apply patches to test systems, and apply patches to production systems. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017595	CIP-007-6	R5.	[REDACTED]	[REDACTED]	1/1/2017	4/28/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED], it had discovered on [REDACTED] it was in noncompliance with CIP-007-6 R5. (5.6.) while it was preparing for an upcoming CIP Audit.</p> <p>This noncompliance started on January 1, 2017 when the entity failed to enforce password changes at least once every 15 calendar months for two Protected Cyber Assets (PCAs). The noncompliance ended on April 28, 2017 when the entity changed the passwords on the two PCAs.</p> <p>Specifically, the entity failed to change the password at least once every 15 calendar months for two switches classified as PCAs. The switches support Disturbance Monitoring Equipment.</p> <p>The root cause of this noncompliance was due to a misunderstanding of the entity's outage request policy and failure to schedule an onsite change within the required timeframe. The SME responsible for the change was under the impression that a three month outage request was needed in order to reset the passwords.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not changing the passwords at least once every 15 calendar months, the devices could be susceptible to password cracking or brute force attacks. If these devices were compromised and an attacker caused them to not report data or report false data that did not correspond to other information, the entity would initiate an investigation. The entity would not perform BES actions on a single point of data.</p> <p>The entity further protected the devices in scope from unauthorized access by locating them within a Physical Security Perimeter and Electronic Security Perimeter. The entity also reviewed the device logs and no unusual events or logins were detected during the noncompliance period.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no relevant underlying causes. NPCC did not consider the entity's compliance history as an aggravating factor in the determination.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <p>1) Changed the password for the devices in scope.</p> <p>To prevent future recurrence the entity:</p> <p>1) updated documents for tracking BESCA to include:</p> <ul style="list-style-type: none"> a) devices with TFE; b) devices that should be remotely manageable; c) device Risk Profile; and <p>2) Created a report with executive review information:</p> <ul style="list-style-type: none"> a) a pivot table that lists the number of password in several categories based on their age. This is now a standard part of the monthly password status report. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017913	CIP-007-6	R5.	[REDACTED]	[REDACTED]	2/1/2017	3/3/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 07, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had discovered on February 10, 2017, it was in noncompliance with CIP-007-6 R5. (5.6.) after conducting an annual review of accounts with interactive access.</p> <p>This noncompliance started on February 1, 2017 when the entity failed to change a shared accounts password within 15 months. The entity last changed the password on October 29, 2015. The shared account is used to perform administration functions for 38 firewalls. The noncompliance ended on March 3, 2017 when the password to the account was changed.</p> <p>The root cause of this noncompliance was lack of a control to ensure password age checks were performed before the entity was in noncompliance.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not performing password changes at least once every 15 calendar months the accounts may become susceptible to brute force attacks or password cracking attacks. The entity reduced the risk of the passwords becoming known to a malicious actor by ensuring only authorized users were given access to the accounts. The accounts cannot be accessed remotely, and the entity actively monitors alerts that would have been generated if a brute force attack had been attempted. After discovering the issue the entity reviewed alerts and none were found to be related to the password for the Shared ID in scope. The entity was out of compliance for a total of thirty three (33) days.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) change Password for the shared ID in scope; 2) developed a plan to implement [REDACTED] (tool that manages passwords); and 3) held monthly meetings to review password status. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018689	CIP-007-6	R4.	[REDACTED]	[REDACTED]	7/1/2016	9/22/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on [REDACTED], it was in noncompliance with CIP-007-6 R4. (4.3., 4.4.) after preparing for an upcoming audit.</p> <p>This noncompliance started on July 1, 2016 when the entity failed to log the required events at the BES Cyber System level or at the Cyber Asset level for one (1) PACS and three (3) BES Cyber Systems. The noncompliance ended on September 22, 2017 when the entity reconfigured its systems and restored the logging functionality or performed manual reviews.</p> <p>Specifically, the entity failed to install its log agent on one PACS server during the initial roll-out of its event log server. The entity further failed to ensure logs for 3 switches classified as BES Cyber Systems were reaching its event log server. The entity discovered through the investigation that the syslog traffic needed to pass through four firewalls and the last firewall in the path was blocking the traffic. The entity was unable to identify when the firewall started blocking the traffic, but identified in audit data from October 2014 that the firewalls were not allowing the traffic.</p> <p>The root cause of this noncompliance was due to control gaps in initial configuration and implementation of the event log system and testing controls on a per change basis, and gaps in quarterly certification process.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not collecting and retaining the required log events, the entity would not be able to perform after the fact investigations into potential cyber security incidents, and the entity would not receive alerts on failed logon attempts. The entity reduced the risk of logon failures and malicious activity going unnoticed by protecting the assets in scope with explicit firewall rules, intrusion detection systems, local antivirus protection for the PACS server, and role based access permissions. The PACS server in scope had no direct access to BES Cyber Systems. All assets in scope are protected from unauthorized physical access.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) verified that other CIP systems were accounted for in logging system (Entity identified scope increase 3 switches); 2) implemented manual monitoring on PACS server in scope; 3) corrected firewall rules for 3 switches to allow syslogs to reach logging system; 4) improved quarterly reviews by incorporating peer oversight controls and formally documenting process; and 5) provided refresher training on revised quarterly review process. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018020482	CIP-005-5	R2.	[REDACTED]	[REDACTED]	7/1/2016	Present	Audit	2/28/2019 Expected Date
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], NPCC determined that [REDACTED] (the entity), as a [REDACTED], was in noncompliance with CIP-005-5 R2. (2.1., 2.3.).</p> <p>This noncompliance started on July 1, 2016 when the entity failed to utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. Additionally, the entity did not require multi-factor authentication for interactive remote access to a PCA within the entity's ESP. The noncompliance will end when the entity completes its mitigation activities.</p> <p>Specifically, the entity identified their corporate DMZ as an ESP. The entity's Intermediate System was logically located within the entity's corporate DMZ. The NERC glossary of terms states that the Intermediate System must not be located inside the ESP. There are no BES Cyber Systems within the corporate DMZ. The Intermediate System in scope includes an [REDACTED] server and a jumphost classified as EACMS. Within the DMZ, the entity has a firewall manager classified as an EACMS and a firewall management switch classified as a PCA.</p> <p>Additionally, the entity did not identify read-only access via a web application to a PCA as Interactive Remote Access. The entity did not afford multi-factor authentication on the read-only connection. Specifically, the entity has a Proxy Server that facilitates the read-only access. The Proxy Server was not identified as an intermediate system and was categorized as an EACMS within an ESP. At the time of the noncompliance, the Proxy Server was logically located within the entity's corporate DMZ which was identified as an ESP.</p> <p>The root cause of this noncompliance was failure to review the NERC glossary of terms when defining its Electronic Security Perimeter, Electronic Access Points, and Intermediate Systems.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, failure to properly define and document applicable systems per the NERC glossary of terms can lead to assets not being identified and protected with the required CIP controls. This can increase the potential vectors a malicious actor can exploit to cause harm to the entity's systems.</p> <p>In this instance, while the entity improperly documented its corporate DMZ as an ESP, it afforded the required protections for assets that were identified as Intermediate Systems. However, the entity failed to identify and require two factor authentication for access to a read-only system within the entity's actual ESP. The read only system is a webserver for remote viewing. It is a read only copy of the entity's EMS server and the read only access can only interact with the Proxy Server in scope that was not identified as an intermediate system, but was identified as an EACMS. The usernames and passwords to the read only system are restricted and must be approved. The usernames for the read only system are not related to the live EMS system, and the read-only web application cannot be reconfigured to access the live system. If the read-only system were to go down, system operations would not be impacted.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no relevant underlying causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) revised ESP Drawing and Asset List, Identify ESPs; and 2) reviewed NERC Glossary of Terms with Staff. <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by February 28, 2019:</p> <ol style="list-style-type: none"> 1) restrict remote firewall management access to [REDACTED]; 2) restrict access to DMZ Firewalls and DMZ firewall manager through established intermediate system ([REDACTED]); and 3) establish Proxy Server as Intermediate System. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018020481	CIP-010-2	R3.	[REDACTED]	[REDACTED]	7/1/2018	10/23/2018	Audit	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted between [REDACTED], NPCC determined that [REDACTED] (the entity), as a [REDACTED], was in noncompliance with CIP-010-2 R3. (3.2.).</p> <p>This noncompliance started on July 1, 2018 when the entity failed to document one or more processes to perform an active vulnerability assessment. The noncompliance ended on October 23, 2018 when the entity updated its Change Management and Vulnerability Assessment document to include a process and procedure for performing an active vulnerability assessment at least once every 36 months.</p> <p>Specifically, the entity had a third party company perform an active vulnerability assessment, but the entity did not have a documented active vulnerability assessment process, and the documentation from the third party did not indicate the methodology that was performed on applicable systems.</p> <p>The root cause of this noncompliance was a failure to review process documentation when the entity engaged a third party to perform the active assessment.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not documenting an active vulnerability assessment process, the entity may not be able to ensure the scope of work for the vulnerability assessment that is performed includes all applicable systems and all applicable requirement parts. The entity reduced the risk of the scope of work of an active vulnerability scan meeting the applicable requirements by having a third party perform the vulnerability scan. In this instance the third party provider was aware of the applicable CIP requirements and performed the required activities.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no relevant underlying causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated Change and Vulnerability Assessment Document; and 2) trained staff on document. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018020483	CIP-005-5	R1.	[REDACTED]	[REDACTED]	7/1/2016	Present	Audit	5/1/2019 Expected Date
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], NPCC determined that [REDACTED] (the entity), as a [REDACTED], was in noncompliance with CIP-005-5 R1. (1.3.).</p> <p>This noncompliance started on July 1, 2016 when the entity failed to include a reason for granting access to inbound and outbound access permissions. The noncompliance will end when the entity completes its mitigation activities to evaluate and reconfigure firewall rules.</p> <p>[REDACTED]</p> <p>The root cause of this noncompliance was lack of vendor documentation and periodic review.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, overly permissive firewall rules can increase the attack vectors and attack surface available to a malicious individual, which could lead to unauthorized access to applicable CIP systems. In this instance, [REDACTED]</p> <p>[REDACTED]</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no relevant underlying causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) followed up with the EMS Vendor; 2) followed up with the Firewall vendor; 3) documented access rules allowing "any" protocol; and 4) installed revised ruleset comments. <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by May 1, 2019:</p> <ol style="list-style-type: none"> 1) evaluate and reconfigure firewall rules for firewall management; 2) evaluate and reconfigure firewall rules for EMS; and 3) perform a final ruleset review. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018020402	CIP-007-6	R2.	[REDACTED]	[REDACTED]	7/1/2016	8/21/2108	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 18, 2018, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it had discovered on August 14, 2018, it was in noncompliance with CIP-007-6 R2. (2.2.) after preparing evidence for an upcoming audit. A PACS support staff member mentioned that a media player was on the list of installed software for PACS workstations. The team immediately recognized that patching for the media player had not been part of the weekly discussions and began investigating the issue.</p> <p>This noncompliance started on July 1, 2016, the enforceable start date of CIP-007-6 R2. The noncompliance ended on August 21, 2018 when the entity evaluated the software security patches in scope.</p> <p>Specifically, the entity failed to evaluate three security patches dating back to as early as February 2015 related to the media player. The media player is used to view stored video. It was installed on ten workstations; five workstations resided at the primary security command center and five resided at the backup security command center.</p> <p>The root cause of this noncompliance was a failure to include the media player in the security patch tracking spreadsheet.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The workstations are protected within a PSP and are located behind network firewalls. These workstations also employ host-based firewalls to control incoming and outgoing network traffic and have anti-malware software installed. Only authorized personnel with authorized physical and cyber access can access the workstations. If logged into the workstation, a user can access the media player to view stored video, launch Microsoft Office applications, or the PACS graphical user interface (GUI). If logged into the PACS GUI, which is a separate user login, depending on their access level, they can watch live/recorded video, monitor/acknowledge security alarms, run reports, and grant/revoke access.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no relevant underlying causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed a review of all installed software to identify any other potential components that were not patched appropriately; 2) presented and approved the media player security patching update to the [REDACTED] which serves as the authority for the approval or rejection of changes to the NERC CIP environments; 3) installed the security patch updates in the PACS test environment and production; and 4) updated the security patching spreadsheet to include security patching tracking for the media player so that future security related patches will be evaluated. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019322	CIP-010-2	R4.	[REDACTED]	[REDACTED]	7/7/2017	10/3/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On March 05, 2018, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on October 3, 2017 it was in noncompliance with CIP-010-2 R4 after performing an electronic access review.</p> <p>This noncompliance started on July 7, 2017 when the entity failed to implement its Transient Cyber Asset plan. Specifically, a contractor connected a non-entity laptop computer to one (1) Medium Impact BES Cyber Asset. The entity's documented plan for Transient Cyber Assets does not allow non-entity laptop computers to be connected to entity cyber assets. The noncompliance ended on October 3, 2017 when the entity discovered the issue and talked to the contractor.</p> <p>The root cause of this noncompliance was inadequate contractor training prior to the April 1, 2017 effective date for CIP-010-2 R4.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not following the entity's Transient Cyber Asset plan to ensure only authorized Transient Cyber Assets are connected to entity cyber assets, the relay in scope could have been infected with malicious software when the contractor connected the unauthorized Transient Cyber Asset to the relay.</p> <p>The entity's contractor reduced the risk of their unauthorized Transient Cyber Asset causing harm to the relay by ensuring patches and antivirus software were up to date. After discovery of the issue the contractor provided the entity with evidence of patching and AV status showing current definitions. The contractor in scope had up-to-date CIP Physical and Cyber Security Training and had an up-to-date Personnel Risk Assessment. The contractor further had authorized physical access and electronic assess to the BES Cyber Assets at five substations.</p> <p>The Medium Impact BES Cyber Asset's at the entity's substations are all firmware based and cannot have third party software installed. The Cyber Assets can only be accessed with the vendor provided software over a serial connection.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reviewed CIP-010-2 R4 requirements with [REDACTED] managers, supervisors, and contractors; and 2) updated training materials (ST.02.04.016 CIP-010 Configuration Change Management and Vulnerability Assessments v1.3). 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019498	CIP-002-5.1a	R2.	[REDACTED]	[REDACTED]	6/22/2017	3/26/2018	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on March 26, 2018 it was in noncompliance with CIP-002-5.1a R2. (2.2.) after preparing Reliability Standard Audit Worksheets for a CIP audit.</p> <p>This noncompliance started on June 22, 2017 when the entity failed to have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 for one (1) Medium Impact facility. The noncompliance ended on March 26, 2018 when the entity had its CIP Senior Manager approve the identifications required by Requirement R1 for the facility in scope.</p> <p>The root cause of this noncompliance was an administrative error. The Medium Impact BES Cyber System [REDACTED] was inadvertently omitted from the CIP Senior Manager approval.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not having the CIP Senior Manager approve the identification required by CIP-002 Requirement R1 they may not afford proper oversight and ensure the appropriate personnel are made responsible for ensuring cyber security controls are applied to the BES Cyber System in scope. Inadequate or non-existent cyber security controls can lead to the compromise or misuse of the BES Cyber System.</p> <p>The entity reduced the risk of inadequate cyber security controls being applied to the BES Cyber System in scope by protecting the system as a Medium Impact BES Cyber System since July 1, 2016. The entity had begun work on its CIP-002 BES Cyber System Categorization for the site in scope on April 28, 2016. The entity has both substation equipment at this location and the HVDC control system. The substation equipment was signed off, but the entity left out the control system document.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <p>1) the entity's CIP Senior Manager approved the identification of the BES Cyber System [REDACTED]</p> <p>To prevent future recurrence, the entity:</p> <p>1) created a GRC task that includes a list of all groups that need to be involved in the annual review, and 2) the CIP Senior Manager signoff form calls out [REDACTED] [REDACTED]</p>					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019393	CIP-008-5	R2.	[REDACTED]	[REDACTED]	7/1/2017	10/19/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED] [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on [REDACTED], it was in noncompliance with CIP-008-5 R2. (2.1) after discussions [REDACTED].</p> <p>This noncompliance started on July 1, 2017, the enforceable start date of the standard. The entity failed to document how their cyber security incident response plan was exercised during NYISO's exercise of a reportable cyber security incident. The noncompliance ended on October 19, 2017, when the entity conducted a cyber security exercise and documented the exercise.</p> <p>The root cause of this noncompliance was a failure to recognize the documentation was inadequate to demonstrate the entity's exercise of their incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The entity participated in the NYISO's exercise of a reportable cyber security incident on November 3, 2016. The entity's documentation of the exercise included an executive summary, exercise overview, exercise design summary, conclusion, observations and recommendations. However, the documentation of the exercise in regard to the entity's cyber security incident response plan was not sufficient.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the required cyber security incident response plan exercise and documentation; and 2) included the entity's compliance group to review the cyber security incident response plan exercise documentation. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018893	CIP-007-6	R1.	[REDACTED]	[REDACTED]	7/1/2016	12/1/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 20, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had discovered it was in noncompliance with CIP-007-6 R1. (1.1.) after performing an annual vulnerability assessment.</p> <p>This noncompliance started on July 1, 2016 when the entity failed to document that it had enabled only logical network accessible ports that it had determined were needed for two (2) Protected Cyber Assets (PCAs) that are associated with a Medium Impact facility. The noncompliance ended on December 1, 2017 when the entity confirmed the two (2) PCAs did not have ports or services opened that were not needed and created the supporting documentation.</p> <p>Specifically, on May 27, 2016 the entity deployed two PCAs with a new control system at a Medium Impact facility. The PCAs could not be managed by the system the entity uses for establishing evidence documentation. The entity should have generated the necessary documentation manually, however, due to an oversight and miscommunication, the documentation was not created.</p> <p>The root cause of this noncompliance was due to lack of oversight and miscommunication during deployment of new assets.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not establishing documentation of open ports and services the entity would not be able to identify changes to the configuration. The entity may also not know that all open ports and services had been validated for need. An enabled port that is not necessary for business purposes could expose the entity's network to software vulnerabilities.</p> <p>The two PCAs are time servers that synchronize time across the entity's network. The entity reduced the risk of an attacker exploiting open ports and services on the two (2) PCAs in scope by placing the servers within an Electronic Security Perimeter within the Medium Impact facility in scope. The Protected Cyber Assets are also located within the entity's Physical Security perimeter which is manned 24x7x365.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <p>1) created ports and services documentation for the two Protected Cyber Assets (time servers).</p> <p>To prevent future recurrence, the entity:</p> <p>1) amended its change control process and checklist to require checkoff/signoff of CIP-007 R1 Controls.</p>					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018101	CIP-005-5	R1.	[REDACTED]	[REDACTED]	7/1/2016	7/17/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 07, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had an issue of CIP-005-5 R1. (1.3). The issue was discovered during an annual vulnerability assessment for the [REDACTED] facility.</p> <p>The noncompliance started on July 1, 2016 when the entity failed to configure an Electronic Access Point with inbound and outbound access permissions, and deny all other access by default. The noncompliance ended on July 17, 2017 when the firewall connection was removed between the [REDACTED] facility and the [REDACTED] substation.</p> <p>[REDACTED]</p> <p>The root cause of the noncompliance was failure to review firewall rules and remove comments after testing was complete. Specifically, the entity commented out some firewalls rules during testing and failed to turn the rules back on during commissioning.</p>					
Risk Assessment			<p>The issue posed a minimal risk to the reliability of the bulk power system. The only way to access the firewall was through the [REDACTED] substation, which is secured by [REDACTED]. Also, the BES Cyber System at [REDACTED] is monitored for changes 24x7 by [REDACTED]. Any changes to the [REDACTED] BES Cyber System are reviewed by [REDACTED] Engineering staff. Authentication (login ID and password) is required into the [REDACTED] PC and authentication (login ID and password) is required into the [REDACTED] gateway servers required for RDP access.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity:</p> <p>1) removed the firewall connection between the [REDACTED] facility and the [REDACTED] substation.</p>					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017899	CIP-010-2	R1.	[REDACTED]	[REDACTED]	11/18/2016	6/26/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on [REDACTED], it was in noncompliance with CIP-010-2 R1. (1.1.) when it was providing baseline evidence [REDACTED].</p> <p>This noncompliance started on November 18, 2016, when the entity installed new security panels and failed to create a baseline document that included device firmware. The noncompliance ended on June 26, 2017, when the security panel baseline spreadsheet was updated with the current firmware version.</p> <p>Specifically, new PACS control nodes and server cabinets were installed as part of an application upgrade, and the entity failed to ensure a baseline document included device firmware. These PACS are associated with High Impact BES Cyber Systems.</p> <p>The root cause of this noncompliance was due to a gap in the change control checklist. Specifically, the change control has a checklist to update documentation but did not specifically call out to verify the baseline was captured.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The firmware version of the two security panels has not changed since the security panels were installed. All PACS are installed within a PSP. Unescorted access to the PSP requires CIP training, PRA and authorization. PACS security panels are installed behind a [REDACTED] Firewall. The [REDACTED] Firewall rules are set to only allow communication from the security panel to the PACS server. There is no remote access capability to the security panel.</p> <p>The default passwords on the security panels are changed and the passwords on the panel are changed at least every 15 months. Cyber access to the panels requires CIP training, PRA and authorization.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <p>1) created baseline for PACS equipment in scope.</p> <p>To prevent future recurrence, the entity:</p> <p>1) set up in GRC a monthly periodic control to review the security panel baseline configurations each month; and 2) updated the security test plan to include a signoff of CIP-010 R1.1.</p>					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019394	CIP-008-5	R2.	[REDACTED]	[REDACTED]	7/1/2017	10/19/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had discovered on [REDACTED], it was in noncompliance with CIP-008-5 R2. (2.1) after discussions [REDACTED].</p> <p>This noncompliance started on July 1, 2017, the enforceable start date of the standard. The entity failed to document how their cyber security incident response plan was exercised during NYISO's exercise of a reportable cyber security incident. The noncompliance ended on October 19, 2017, when the entity conducted a cyber security exercise and documented the exercise.</p> <p>The root cause of this noncompliance was a failure to recognize the documentation was inadequate to demonstrate the entity's exercise of their incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The entity participated in the NYISO's exercise of a reportable cyber security incident on November 3, 2016. The entity's documentation of the exercise included an executive summary, exercise overview, exercise design summary, conclusion, observations and recommendations. However, the documentation of the exercise in regard to the entity's cyber security incident response plan was not sufficient.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the required cyber security incident response plan exercise and documentation; and 2) included the entity's compliance group to review the cyber security incident response plan exercise documentation. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019359	CIP-007-6	R5.	[REDACTED]	[REDACTED]	7/1/2016	3/5/2018	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had discovered on [REDACTED], it was in noncompliance with CIP-007-6 R5. (5.5.) after it selected a random sampling of relays to verify compliance attributes [REDACTED].</p> <p>This noncompliance started on July 1, 2016 when the entity failed to meet the minimum password length and/or complexity requirements for 79 devices. The noncompliance ended on March 5, 2018, when the entity took actions on validating and implementing the password requirements.</p> <p>[REDACTED]</p> <p>The root cause of this noncompliance was failure to comply with their password guidelines/procedures.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, the risk was minimized because the passwords had been changed from their default values, the relays must be physically accessed to modify system settings (no ERC), and the relays are protected by [REDACTED].</p> <p>No harm is known to have occurred as a result of this issue of non-compliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) held a training session to communicate the NERC CIP-007 R5.5 requirements regarding password length and complexity with relevant staff; 2) updated their relay password sheet to include the NERC CIP requirement language for password length and complexity in the [REDACTED] department at [REDACTED]; 3) reviewed and revised the CIP Request/Work Order templates to ensure that the technicians are clearly advised of the NERC CIP standard requirement language; and 4) reviewed password parameters at all [REDACTED] locations and took actions on validating and implementing the password requirements. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017599	CIP-004-6	R4.	[REDACTED]	[REDACTED]	8/12/16	10/31/2016	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On May 16, 2017, [REDACTED] (the entity) submitted a Self-Log stating that, as a [REDACTED], it had discovered on September 15, 2016 (Instance 1), October 6, 2016, (Instance 2), and October 31, 2016 (Instance 3) it was in noncompliance with CIP-004-6 R4.</p> <p>The first instance of noncompliance began on September 15, 2016, when the entity did not follow their process to authorize unescorted physical access into a PSP based on need. The noncompliance ended the same day on September 15, 2016, when unescorted physical access was removed. In this instance a government inspector who had access failed to comply with the entity's internal annual PRA requirements which resulted in the inspector's access being revoked. The Entity's Security Staff failed to recognize that the access was revoked and issued an onsite badge which provided unescorted physical access for the duration of the inspection. The entity failed to reauthorize the government inspector per the Entity's documented access authorization process.</p> <p>The root cause of the noncompliance was due to not following procedure.</p> <p>The second instance of noncompliance began on October 6, 2016 when security staff issued a temporary card key with access rights in excess of an employee's approved access rights. The noncompliance ended on October 7, 2016 when the employee returned the temporary card key.</p> <p>The root cause of the noncompliance was due to not following procedure and incorrectly granting of access in the system of record from the authorization approval.</p> <p>The third instance of noncompliance began on August 12, 2016 when security staff granted unescorted physical access to the wrong employee due to both employees having the same last name. The noncompliance ended on October 31, 2016 when access was corrected in the PACS system to reflect the employees' approved accesses. The entity discovered the noncompliance while removing access rights during the transfer of the employee with the incorrect access. Both employees have authorized access to Physical Security Areas, including the requisite valid Personal Risk Assessments and Cyber Security Training certifications but the access rights were misapplied to their credentials.</p> <p>The root cause of the noncompliance was due to not following procedure and incorrectly granting of access in the system of record from the authorization approval.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>In each instance all users had valid Personal Risk Assessments and Cyber Security Training certifications in accordance with the NERC CIP Standards.</p> <p>In instance 1, the noncompliance duration was less than a day and the areas where the individual accessed was continuously occupied. Additionally, the Government Inspector had his access revoked due to company PRA policy which removes access to contractors when PRA dates exceeds one year. Per CIP-004-6 R3.5 a PRA is required to be completed within the last seven years. The Government Inspector had up-to-date CIP training.</p> <p>In instance 2, the employee did not use the temporary key card to enter or attempt to enter any PSPs in excess of his authorization profile throughout the duration of the noncompliance. The badge was returned to security within twenty four hours of the temporary badge being issued.</p> <p>In instance 3, both employees have authorized access to PSAs, including the requisite valid Personal Risk Assessments and Cyber Security Training certifications. The employee did not access the PSP during the duration of the noncompliance.</p> <p>No harm is known to have occurred as a result of these issues of non-compliance.</p>					
Mitigation			<p>To mitigate this issue for Instance 1, the entity:</p> <ol style="list-style-type: none"> 1) identified the issue and immediately removed the unauthorized access; 2) reviewed the applicable entity procedures and expectations for issuance of access rights to PSPs; 3) submitted and approved physical access request to the control room for the involved government inspector; 4) met with the [REDACTED] Security staff regarding the applicable physical access procedures and their implementation for managing physical access to areas containing BES Cyber Systems; and 5) provided reinforcement training on the applicable procedures to the Facility security staff responsible for managing physical access to areas containing BES Cyber Systems. <p>To mitigate this issue for Instance 2, the entity:</p>					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017599	CIP-004-6	R4.	[REDACTED]	[REDACTED]	8/12/16	10/31/2016	Self-Log	Completed
			<p>1) identified the issue and removed the unauthorized access on the spare card key; 2) spoke with the security staff involved in the incident and reviewed the applicable [REDACTED] procedures and expectations for issuance of access rights to PSPs; 3) met with the Facilities security managers regarding the applicable physical access procedures and their implementation for managing physical access to areas containing BES Cyber Systems; 4) provided instruction on the logging of all the required information for issuing card keys; 5) provided instruction on the logging of all the required information on the Command Post 2- Key and Spare Card Key Log to security staff responsible for the issuance of temporary physical access card keys; and 6) provided reinforcement training on the applicable procedures to the Facility security staff responsible for managing physical access to areas containing BES Cyber Systems.</p> <p>To mitigate this issue for Instance 3, the entity:</p> <p>1) identified the issue and removed the unauthorized access on the spare card key; 2) reviewed the applicable [REDACTED] procedures and expectations for issuance of access rights to PSPs with the security staff involved in the incident; 3) met with the Facilities security managers regarding the applicable physical access procedures and their implementation for managing physical access to areas containing BES Cyber Systems; 4) provided reinforcement training on the applicable procedures to the Facility security staff responsible for managing physical access to areas containing BES Cyber Systems; and 5) conducted an evaluation on the feasibility and options on implementing an enhanced Auditing and Reporting Module on the applicable Physical Access Control Systems.</p>					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018298	CIP-007-6	R4.	[REDACTED]	[REDACTED]	7/1/2016	10/20/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 1, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had discovered on March 9, 2017 it was in noncompliance with CIP-007-6 R4. (4.1.) after a relay technician discovered, upon reviewing the relay job plans, that the instructions in the job plan were incomplete to provide the Schweitzer SEL 300 Series relay's full security event logging capabilities.</p> <p>This noncompliance started on July 1, 2016 when the entity failed to log events at the BES Cyber System level or at the Cyber Asset level per System/Cyber Asset capability for detected successful and failed access attempts for 70 Relays. The noncompliance ended on October 20, 2017 when the entity updated the logging capability settings of each relay to meet the requirements of CIP-007-6 R4.1.</p> <p>Specifically, the entity's documented process did not include details to enable security event logging for SEL relays. The entity confirmed that only 7 of 77 relays had security event logging enabled.</p> <p>The root cause of this noncompliance was the documented process established for SEL relays under CIP-007-6 R4.1 was deficient and did not explicitly mention the detailed instructions to enable security event logging per the device's fullest capabilities.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, the entity may not have situational awareness of a potential threat by failing to log applicable cyber security events. The relays in scope are protective relays that can cause a circuit breaker to operate. The entity would not be able to use device logs to perform after the fact investigations of relay misoperations to identify if the misoperation was due to unauthorized electronic access.</p> <p>[REDACTED]</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the logging capability of each relay; 2) updated the relay job plans to enable login events and verify that login attempts are captured; and 3) validate logging capabilities of the remaining relays to identify if a relay does not meet the requirements of R4.1. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018296	CIP-004-6	R5.	[REDACTED]	[REDACTED]	5/16/2017	5/17/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 1, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had discovered on May 17, 2017 it was in noncompliance with CIP-004-6 R5. (5.1.) after it followed-up on a termination request it received on May 16, 2017 and discovered that an individual was actually released by the vendor in the afternoon of May 15th, 2017.</p> <p>This noncompliance started on May 16, 2017 when the entity failed to initiate removal of one individual's unescorted physical access and interactive remote access within 24 hours of their termination action. The noncompliance ended on May 17, 2017 when the entity revoked the individual's unescorted physical access and interactive remote access.</p> <p>Specifically, the entity's vendor terminated one individual on May 15, 2017 due to a projected reduction in business (i.e. laid-off). The vendor did not send notification to the entity until May 16, 2017. The estimated lag between when physical and remote system access was revoked, versus when that access should have been revoked, was approximately 13 hrs. (37 rather than the required 24 hours).</p> <p>The root cause of this noncompliance was lack of a control to ensure timely termination notifications from vendors.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not terminating unescorted physical access and interactive remote access upon a termination action, terminated individuals may access BES Cyber Systems with the intent to misuse or disrupt operations.</p> <p>The entity reduced the risk of the terminated employee gaining access to systems after their termination by not providing the individual with an active card-key for 24/7 use. The entity provides contractors with a temporary card-key upon arrival for unescorted access. In order to obtain access, the individual would have to present themselves to the entity's site security where the person's identity and access authorizations would be reviewed. Then, site security identifies and contacts the individual's point-of-contact to advise that the contractor is onsite.</p> <p>Also, during the noncompliance period the individual did not possess an authorized laptop and [REDACTED] to initiate remote system access. The equipment issued to the vendor for that purpose was in the possession of another contract employee who was fully authorized by the entity for such access, and who was not affected by the vendor's employment layoffs.</p> <p>According to the PACS logs, the last time the individual in scope had physical access to the entity's PSP's was on May 5, 2017.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reinforced the employment based 24-hour revocation requirement with the vendors and [REDACTED] point of contacts; and 2) reviewed the contract language to ensure vendor responsibility in regards to [REDACTED] notification in a timely manner. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018297	CIP-006-6	R1.	[REDACTED]	[REDACTED]	12/19/2016	4/6/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 1, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on March 31, 2017 it was in noncompliance with CIP-006-6 R1. (1.9.) after conducting an investigation of a possible incident involving unauthorized access into a protected area.</p> <p>This noncompliance started on December 19, 2016 when the entity failed to configure a PACS server to retain physical access logs of individuals with authorized unescorted physical access, into each PSP for at least ninety calendar days. The noncompliance ended on April 6, 2017 when the entity had its vendor configure the PACS server to retain physical access logs for at least ninety calendar days.</p> <p>Specifically, the entity installed the PACS server in mid-December 2016 and the server was configured to only retain 30 days of logs. The period in which the missing records was from December 19, 2016 to February 28, 2017 (inclusive). During that period, the only backup of the access records are hard-copy printouts of all 'Failed Access' attempts (resulting from the daily manual log reviews). As a result, there are no automated records available for 60 of the 90 days of access records required by the NERC CIP Standard.</p> <p>The root cause of this noncompliance was lack of compliance oversight and controls to ensure new PACS are configured to meet the requirements upon onboarding.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not retaining physical access logs of entry into each PSP for at least ninety calendar days, the entity could not use the logs to perform after-the-fact investigations. This could hinder its ability to identify potential individuals involved in security incidents or device misuse.</p> <p>The entity reduced the risk of not being able to identify potential insider threat incidents by actively reviewing all access into, and out of, all protected areas on a daily basis (although hard-copy reports of that review are only printed and retained for instances of 'Failed Access' attempts). During the period in which the PACS logging was not enabled, there were no instances where improper access was noted.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reconfigured the PACS to retain logs for at least 90 days; 2) verified access log retention period during annual PACS maintenance; and 3) will explore creation of a checklist and/or procedure for final site validation upon acceptance of a PACS installation. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019395	CIP-008-5	R2.	[REDACTED]	[REDACTED]	7/1/2017	10/19/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had discovered on [REDACTED], it was in noncompliance with CIP-008-5 R2. (2.1) [REDACTED].</p> <p>This noncompliance started on July 1, 2017, the enforceable start date of the standard. The entity failed to document how their cyber security incident response plan was exercised during NYISO's exercise of a reportable cyber security incident. The noncompliance ended on October 19, 2017, when the entity conducted a cyber security exercise and documented the exercise.</p> <p>The root cause of this noncompliance was a failure to recognize the documentation was inadequate to demonstrate the entity's exercise of their incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The entity participated in the NYISO's exercise of a reportable cyber security incident on November 3, 2016. The entity's documentation of the exercise included an executive summary, exercise overview, exercise design summary, conclusion, observations and recommendations. However, the documentation of the exercise in regard to the entity's cyber security incident response plan was not sufficient.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the required cyber security incident response plan exercise and documentation; and 2) included the entity's compliance group to review the cyber security incident response plan exercise documentation. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017892	CIP-007-6	R5.	[REDACTED]	[REDACTED]	7/1/2016	3/3/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 07, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had discovered on February 9, 2017 it was in noncompliance with CIP-007-6 R5. (5.6.) after performing its annual review of accounts with interactive access.</p> <p>This noncompliance started on July 1, 2016, when the entity failed to change the passwords at least once every 15 calendar months for six (6) shared IDs that had access to a combined total of 134 High Impact BES Cyber Assets and associated EACMS. The noncompliance ended on March 3, 2017 when the entity changed the passwords of the six (6) shared IDs.</p> <p>Specifically, the six (6) shared IDs are local accounts that are not part of the domain and do not have a set expiration date. The six (6) shared IDs had the following access:</p> <ol style="list-style-type: none"> 1. Account 1 had access to 37 of 39 servers, was last changed 11/6/2015 2. Account 2 had access to 2 servers, was last changed 11/6/2015 3. Account 3 had access to 42 of 57 workstations, was last changed 11/6/2015 and 1 workstation was last changed 4/29/2013 4. Account 4 had access to 14 switches, was last changed 11/4/2015 5. Account 5 had access to 14 switches, was last changed 11/4/2015 6. Account 6 had access to 38 firewalls, was last changed 10/29/2015 <p>The root cause of this noncompliance was due to lack of a control to ensure password age checks were performed before the entity was in noncompliance.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not performing password changes at least once every 15 calendar months the accounts may become susceptible to brute force attacks or password cracking attacks. The entity reduced the risk of the passwords becoming known to a malicious actor by ensuring only authorized users were given access to the accounts. The accounts cannot be accessed remotely, and the entity actively monitors alerts that would have been generated if a brute force attack had been attempted. After discovering the issue, the entity reviewed alerts and found no alerts related to the passwords for the six (6) shared IDs in scope.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) changed passwords for the six (6) shared IDs in scope; 2) developed a plan to implement [REDACTED] (tool that manages passwords); and 3) held monthly meetings to review password status. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017893	CIP-002-5.1	R1.	[REDACTED]	[REDACTED]	7/1/2016	5/9/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 19, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on November 3, 2016, it was in noncompliance with CIP-002-5.1 R1. The issue was discovered after a control center operator brought a pump house issue to light during a compliance work plan meeting.</p> <p>This noncompliance started on July 1, 2016, when the entity miscategorized [REDACTED]. The entity originally categorized the assets as low impact. Specifically, [REDACTED]. The noncompliance ended on May 9, 2017 when the entity categorized the fifteen pump houses as Medium Impact BES Cyber Assets.</p> <p>The root cause is due to a misunderstanding in how the equipment was being used to monitor and control the BES.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify BES Cyber Systems as applicable to the CIP Standards, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The entity reduced the risk of the Cyber Assets not being afforded CIP protections by identifying the assets as Medium Impact per CIP-002-5.1 Attachment 1 Section 2.6 and in some cases Sections 2.5 and 2.7. While the entity failed to identify the classification of the Cyber Assets related to the [REDACTED], it did afford the following CIP protections: Security Awareness, Security Patch Management, Malicious Code Prevention measures, Security Event Monitoring, identification and inventory of all known enabled default or other generic account types. The entity also changed known default passwords and implemented passwords that met complexity requirements. The entity included the asset in its Cyber Security Incident Response Plan, had documented recovery plans, had established a baseline configuration, and implemented configuration change management processes. The entity also included the BES Cyber Assets in scope in a paper or active vulnerability assessment and had developed a Transient cyber Asset and Removable Media process.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) conducted station walk-downs to inventory BES Cyber Assets at each [REDACTED] location; and 2) updated the Asset list and official database for components. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017894	CIP-004-6	R4.	[REDACTED]	[REDACTED]	3/29/2017	4/12/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 07, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had discovered on April 12, 2017 it was in noncompliance with CIP-004-6 R4. after IT Personnel identified multiple alerts on failed logins to a PACS workstation.</p> <p>This noncompliance started on March 29, 2017, when the entity failed to ensure a new contractor (Contractor 1) had completed the NERC CIP Training prior to accessing a PACS system associated with High and Medium Impact BES Cyber Systems. The noncompliance ended on April 12, 2017, when the entity changed the password on the account.</p> <p>Specifically, an authorized contractor (Contractor 2) allowed their login credentials to be used by Contractor 1 to access the PACS. The account had read-only access to the PACS and the ability to open Physical Security Perimeter (PSP) access control doors. The issue was identified through a monitoring system that alerted on failed login attempts. Upon an investigation of the failed login attempts, the entity identified the utilization of Contractor 2's login credentials by Contractor 1.</p> <p>The root cause was a failure to enforce policy. Contractor 2 did not follow the access approval process before allowing access to the PACS. The process was for a contract security guard to work with a CIP-cleared guard, during on-the-job training, until the contractor had been fully CIP-cleared (PRA and CIP training) and access request processed.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Electric System (BES). Specifically, sharing account passwords with unauthorized individuals could lead to the compromise of the cyber asset and other cyber assets on the network. The exposure of malicious activity by an unauthorized individual was limited to the entity's PACS. The PACS does not allow cyber access to any other BES Cyber Systems or assets. The account in scope had read-only access to the PACS and did not have the ability to change individual access profiles or door enrollments. However, it did have the capacity to open PSP doors. The entity reviewed the security event logs for the seven (7) nights, during which the new contractor worked alone, and no invalid or unauthorized access attempts were recorded, The contractor did not open any CIP PSP doors remotely. System Security only grants unescorted access to BES Cyber Systems or assets after the individual has completed a PRA and CIP Training. Furthermore, the entity's process defines and implements a process to detect, identify, and log security events. The entity's CIP-003 Cyber Security Policy requires the documentation and implementation of a process to log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of detected events: Successful login attempts; Failed access attempts and failed login attempts. On the date the incident was discovered, the entity's IT Security received numerous alerts on failed login attempts to the PACS workstation and promptly responded and corrected the incident. An investigation confirmed that this individual accessed no other CIP systems. The contractor in scope had a recent PRA and was only able to gain access to the PACS workstation using another contractors login credentials. Since the noncompliance, the contractor has completed the CIP training and has been granted access to the PACS.</p> <p>No harm is known to have occurred as a result of this issue of non-compliance.</p>					
Mitigation			<p>To mitigate this issue, the entity:</p> <ol style="list-style-type: none"> 1) changed the password to the account in scope; 2) assigned IT Security Awareness Fundamentals training to all security guards in the Learning Management System; <ol style="list-style-type: none"> i) This security awareness training course covers key security best practices end users should follow so they can prevent, detect, and respond to information security threats. It is designed to cover all of the essential topics such as password management, identity theft, malware, social engineering, phishing, physical security, travel safety, mobile data, privacy and acceptable use. 3) ensure that all personnel are aware that it is against Company policy to share login credentials to access Systems, whether CIP or Corporate. This was sent to all guards via email; and 4) ensure that, as part of the on-boarding process, PRA and CIP Training are completed for personnel, including contractors, on their start date/first day on the job. This was achieved by creating a document which includes steps for onboarding a new security guard in order to prevent the recurrence of having a new guard begin their on-the-job training without being CIP-cleared. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017896	CIP-010-2	R2.	[REDACTED]	[REDACTED]	8/6/2016	4/4/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 07, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had discovered on April 4, 2017 it was in noncompliance with CIP-010-2 R2. (2.1.) after its [REDACTED] team discovered the issue during the required monthly monitoring review.</p> <p>This noncompliance started on August 6, 2016 when the entity failed to monitor one (1) High Impact BES Cyber System at least once every 35 calendar days for changes to the baseline configuration, as required by CIP-010-2 R2, Part 2.1. The noncompliance ended on April 4, 2017 when the entity reviewed the baseline for changes.</p> <p>The root cause of this noncompliance was due to lack of a control to ensure all assets on the entity's CIP-002 master list had been manually monitored for baseline changes.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose serious or substantial risk to the reliability of the bulk power system. Specifically, by not monitoring the High Impact Cyber Asset for changes, potentially malicious changes or unauthorized changes would have gone unnoticed by the entity. The High Impact Cyber Asset in scope is a Remote Desktop Protocol Workstation that is a dispatch machine in the Control Center. The workstation itself does not have the ability to control the grid. The entity reduced the risk of potentially unauthorized or malicious changes occurring on this workstation by affording it the other CIP protections that are defined in the standard. The workstation has been on the entity's CIP-002 list since July 1, 2016. The entity reviewed the asset in scope to determine if there were any changes to the baseline configuration and there were none. The entity also reviewed its entire asset list and found no other issues with monitoring assets for changes to the baseline.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reviewed the asset to determine if there were any changes to the baseline configuration detected. The review resulted in no changes detected; 2) reviewed CIP asset list to ensure no other CIP asset was omitted from monitoring process; 3) coached individual that performs monitoring task; 4) enhanced procedure CIP-010-PRO-02 to ensure baseline configuration data is reviewed every 35 calendar days as required; and 5) included CIP-002 asset list in monthly manual monitoring process. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017897	CIP-006-6	R1.	[REDACTED]	[REDACTED]	7/1/2016	6/27/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 7, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had an issue of CIP-006-6 R1. The issue was discovered after a control center operator brought a pump house issue to light during a compliance work plan meeting on November 3, 2016. During an extent of condition review, the entity discovered on March 27, 2017, it had commissioned two control houses without a proper Physical Security Perimeter (PSP).</p> <p>This noncompliance started on July 1, 2016, when the entity failed to define operational or procedural controls to restrict physical access to two (2) control houses and [REDACTED] pump houses. The PSPs in scope are Medium Impact without External Routable Connectivity. The noncompliance ended on June 27, 2017, when the entity defined operational or procedural controls within its Physical Security Plan for the PSPs in scope.</p> <p>[REDACTED]</p> <p>The root cause of the noncompliance was determined to be incomplete design documentation.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not defining operational or procedural controls to restrict physical access to applicable systems, the entity may not afford controls to restrict physical access. Not protecting PSPs could result in unauthorized access, misoperation, or damage to the Medium Impact BES Cyber Systems in scope, which could jeopardize the reliable operation of BES assets. [REDACTED]</p> <p>[REDACTED]</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) classified the pump house facilities as Medium Impact Assets; 2) conducted station walk-downs to inventory of BES Cyber Assets at each pump house location; 3) [REDACTED] 4) conducted an inspection of all substations coupled with a review of the NERC Standards determined the potential of non-compliance issues are limited to only two (2) control houses; 5) installed physical security controls as required by the entity's Physical Security Plan; and 6) formalized an engineering practice to help ensure physical security controls are installed at BES facilities. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018432	CIP-007-6	R4.	[REDACTED]	[REDACTED]	7/1/2016	9/22/2017	Audit	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], NPCC determined that [REDACTED] (the entity), as a [REDACTED] was in noncompliance with CIP-007-6 R4; SR4.3.</p> <p>This noncompliance started on July 1, 2016 when the entity failed to log the required events at the BES Cyber System level or at the Cyber Asset level for one (1) PACS and three (3) BES Cyber Systems. The noncompliance ended on September 22, 2017 when the entity reconfigured its systems and restored the logging functionality or performed manual reviews.</p> <p>Specifically, the entity failed to install its log agent on one PACS server during the initial roll-out of its event log server. The entity further failed to ensure logs for 3 switches classified as BES Cyber Systems were reaching its event log server. The entity discovered through the investigation that the syslog traffic needed to pass through four firewalls and the last firewall in the path was blocking the traffic. The entity was unable to identify when the firewall started blocking the traffic, but identified in audit data from October 2014 that the firewalls were not allowing the traffic.</p> <p>The root cause of this noncompliance was due to control gaps in initial confirmation and implementation of the event log system and testing controls on a per change basis, and gaps in quarterly certification process.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not collecting and retaining the required log events, the entity would not be able to perform after the fact investigations into potential cyber security incidents, and the entity would not receive alerts on failed logon attempts.</p> <p>The entity reduced the risk of logon failures and malicious activity going unnoticed by protecting the assets in scope with explicit firewall rules, intrusion detection systems, local antivirus protection for the PACS server, and role based access permissions. The PACS server in scope had no direct access to BES Cyber Systems. All assets in scope are protected from unauthorized physical access.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>The entity has five previous violations of CIP-007. NPCC determined that the entity's compliance history should not serve as a basis for applying a penalty. There was a different underlying cause for each of the prior violations.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) verified that other CIP systems were accounted for in logging system (Entity identified scope increase 3 switches); 2) implemented manual monitoring on PACS server in scope; 3) corrected firewall rules for 3 switches to allow syslogs to reach logging system; 4) improved quarterly reviews by incorporating peer oversight controls and formally documenting process; and 5) provided refresher training on revised quarterly review process. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017914	CIP-007-6	R5.	[REDACTED]	[REDACTED]	2/1/2017	3/3/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 07, 2017, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on February 10, 2017, it was in noncompliance with CIP-007-6 R5. (5.6.) after conducting an annual review of accounts with interactive access.</p> <p>This noncompliance started on February 1, 2017 when the entity failed to change a shared accounts password within 15 months. The entity last changed the password on October 29, 2015. The shared account is used to perform administration functions for 38 firewalls. The noncompliance ended on March 3, 2017 when the password to the account was changed.</p> <p>The root cause of this noncompliance was lack of a control to ensure password age checks were performed before the entity was in noncompliance.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not performing password changes at least once every 15 calendar months the accounts may become susceptible to brute force attacks or password cracking attacks. The entity reduced the risk of the passwords becoming known to a malicious actor by ensuring only authorized users were given access to the accounts. The accounts cannot be accessed remotely, and the entity actively monitors alerts that are generated if a brute force attack had been attempted. After discovering the issue, the entity reviewed alerts and none were found to be related to the password for the Shared ID in scope. The entity was out of compliance for a total of 33 days.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) changed the password for the shared ID in scope; 2) developed a plan to implement [REDACTED] (tool that manages passwords); and 3) held monthly meetings to review password status. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018688	CIP-007-6	R4.	[REDACTED]	[REDACTED]	7/1/2016	9/22/2017	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on [REDACTED], it was in noncompliance with CIP-007-6 R4. (4.3., 4.4.) after preparing for an upcoming audit.</p> <p>This noncompliance started on July 1, 2016 when the entity failed to log the required events at the BES Cyber System level or at the Cyber Asset level for one (1) PACS and three (3) BES Cyber Systems. The noncompliance ended on [REDACTED] when the entity reconfigured its systems and restored the logging functionality or performed manual reviews.</p> <p>Specifically, the entity failed to install its log agent on one PACS server during the initial roll-out of its event log server. The entity further failed to ensure logs for three switches classified as BES Cyber Systems were reaching its event log server. The entity discovered that the syslog traffic needed to pass through four firewalls and the last firewall in the path was blocking the traffic. The entity was unable to identify when the firewall started blocking the traffic, but identified in audit data from [REDACTED] that the firewalls were not allowing the traffic.</p> <p>The root cause of this noncompliance was due to control gaps in initial configuration and implementation of the event log system and testing controls on a per change basis, and gaps in quarterly certification process.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not collecting and retaining the required log events, the entity would not be able to perform after the fact investigations into potential cyber security incidents, and the entity would not receive alerts on failed logon attempts. The entity reduced the risk of logon failures and malicious activity going unnoticed by protecting the assets in scope with explicit firewall rules, intrusion detection systems, local antivirus protection for the PACS server, and role based access permissions. The PACS server in scope had no direct access to BES Cyber Systems. All assets in scope are protected from unauthorized physical access.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) verified that other CIP systems were accounted for in logging system (Entity identified scope increase 3 switches); 2) implemented manual monitoring on PACS server in scope; 3) corrected firewall rules for 3 switches to allow syslogs to reach logging system; 4) improved quarterly reviews by incorporating peer oversight controls and formally documenting process; and 5) provided refresher training on revised quarterly review process. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018020575	CIP-002-5.1a	R2.	[REDACTED]	[REDACTED]	6/24/2018	9/12/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 23, 2018, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED], it had discovered on September 11, 2018 it was in noncompliance with CIP-002-5.1a R2. (2.1., 2.2.) after the Chief Engineer began pressing its subject matter experts and consultants for compliance status.</p> <p>This noncompliance started on June 24, 2018 when the entity failed to approve the identifications required by R1 at least once every 15 calendar months for low impact BES Cyber Systems. The noncompliance ended on September 12, 2018 when the entity's CIP Senior Manager reviewed and approved the identification required by R1.</p> <p>The root cause of this noncompliance was a lack of a control to ensure reviews were performed prior to the compliance due date.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not periodically conducting a review of BES Cyber Systems and their associated BES Cyber Assets the entity may fail to identify new BES Cyber Systems and ensure the systems are afforded the appropriate level of cyber security.</p> <p>While the entity failed to perform a timely review of its low impact BES Cyber Systems, the entity's policies and procedures to comply with the CIP Standards were in place and the low impact BES Cyber Systems were afforded the required physical and electronic access controls. No new BES Cyber Systems were identified when the entity performed its review.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reviewed and approved an updated CIP-002 Asset list by the CIP Senior Manager; 2) revised its CIP-003 policy to include 15-month review tracking; 3) created a calendar entry to notify appropriate personnel of the need to complete the CIP-002 annual assessments; and 4) trained appropriate personnel on the new policy for CIP-002 tracking. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019214	CIP-007-6	R4	[REDACTED]	[REDACTED]	12/27/2017	2/7/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 12, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R4.</p> <p>This noncompliance involves three instances.</p> <p>In each instance, the entity was one day late in completing its log summary review. The entity discovered these instances through its internal control, its bi-weekly security event log review. In the first instance, the review should have been completed by December 26, 2017, but was not completed until the next day. The entity identified this instance on December 27, 2017. In the second instance, the review should have been completed by January 12, 2018, but was not completed until the next day. The entity identified this instance on January 15, 2018. In the third instance, the review should have been completed by February 6, 2018, but was not completed until the next day. The entity identified this instance on February 7, 2018.</p> <p>The root cause was an ineffective preventative control. The control at the time of the instances consisted of a bi-weekly review task and was designed for subject matter experts to complete the review on a specified day of the week (bi-weekly), which are 14 days apart to remain within the 15 calendar day interval. However, if a review was completed more than one day early in a previous cycle (which was the case here) and then on the due date in next cycle, the 15 day interval was violated. This noncompliance involves the management practice of verification, which involves ensuring that tasks are completed as required, including within the required time.</p> <p>The duration of each instance was one day. This noncompliance started on December 27, 2017, which, in the first instance, is the day after the review should have been completed, and ended on February 7, 2018, when, in the last instance, the review was complete.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The purpose of reviewing event logs is to potentially identify security incidents that the entity did not otherwise identify through real-time alerts. Thus, the potential risk of not timely reviewing event logs is that security incidents may go unidentified, leaving the entity's system at risk of compromise. This risk is reduced here because the entity reviewed the logs only one day late, and the entity quickly identified the instances through its biweekly detective control. Accordingly, the noncompliance posed only minimal risk to the reliability of the BPS. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance and violations involved different root causes than the current noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the Security Event Log Reviews that were outside the required 15 day interval; 2) confirmed and documented back-ups to perform the Security Event Log Reviews so that primary and back-up subject matter experts are directly contacted regarding the need to review the log review prior to the required 15 day interval; 3) performed an extent of condition review for the bi-weekly security event log reviews to determine if any other security event log reviews were completed outside of the required 15 day interval; and 4) increased the frequency of the existing preventative control to a weekly review of security event logs which will prevent the reviews from being completed outside the 15 day interval and to ensure compliance with the Requirement. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018650	CIP-007-6	R4	[REDACTED]	[REDACTED]	10/7/2017	2/7/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On November 2, 2017, and February 12, 2018, [REDACTED] submitted Self-Reports stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R4. Additionally, on February 16, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R4. ReliabilityFirst initially assigned Violation ID RFC2018019260 to that Self-Report, but then administratively dismissed RFC2018019260 and is instead resolving that matter under RFC2017018650. This noncompliance involves four instances.</p> <p>In the first instance, on October 10, 2017, as a result of the entity's bi-weekly security event log review internal control, the entity's IT [REDACTED] Team discovered that its Transmission team's review of a summarization of logged events was completed four days past the 15 days required by the Standard. The review should have been completed by October 6, 2017.</p> <p>In the second, third, and fourth instances, the entity was one day late in completing its log summary review. The entity discovered these instances through its internal control, its bi-weekly security event log review. In the second instance, the review should have been completed by December 26, 2017, but was not completed until the next day. The entity identified this instance on December 27, 2017. In the third instance, the review should have been completed by January 12, 2018, but was not completed until the next day. The entity identified this instance on January 15, 2018. In the fourth instance, the review should have been completed by February 6, 2018, but was not completed until the next day. The entity identified this instance on February 7, 2018.</p> <p>Regarding the first instance, the root cause was that the individual tasked with completing the review was out of the office for most of the review period and a back-up was not assigned, as required by the entity's process. This involves the management practice of work management, which includes ensuring proper resources are available to perform required tasks.</p> <p>Regarding the second, third, and fourth instances, the root cause was an ineffective preventative control. The control at the time of the instances consisted of a bi-weekly review task and was designed for subject matter experts to complete the review on a specified day of the week (bi-weekly), which are 14 days apart to remain within the 15 calendar day interval. However, if a review was completed more than one day early in a previous cycle (which was the case here) and then on the due date in next cycle, the 15 day interval was violated. This noncompliance involves the management practice of verification, which involves ensuring that tasks are completed as required, including within the required time.</p> <p>The duration of each instance was between one and three days. This noncompliance started on October 7, 2017, which, in the first instance, is the day after the review should have been completed, and ended on February 7, 2018, when, in the last instance, the review was complete.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The purpose of reviewing event logs is to potentially identify security incidents that the entity did not otherwise identify through real-time alerts. Thus, the potential risk of not timely reviewing event logs is that security incidents may go unidentified, leaving the entity's system at risk of compromise. This risk is reduced here because the entity reviewed the logs between only one and three days late, and the entity quickly identified the instances through its biweekly detective control. Accordingly, the noncompliance posed only minimal risk to the reliability of the BPS. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance and violations involved different root causes than the current noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the Security Event Log Reviews that were outside of the required 15 day interval; 2) confirmed and documented back-ups to perform the Security Event Log Reviews so that primary and back-up subject matter experts are directly contacted regarding the need to review the log review prior to the required 15 day interval; 3) performed an extent of condition review for the bi-weekly security event log reviews to determine if any other security event log reviews were completed outside of the required 15 day interval; and 4) increased the frequency of the existing preventative controls to a weekly review of security event logs which will prevent the reviews from being completed outside of the 15 day interval and to ensure compliance with the Requirement. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2015015373	CIP-003-3	R6	[REDACTED]	[REDACTED]	8/12/2015	10/16/2015	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On November 19, 2015, the entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-003-3 R6. On February 26, 2016, the entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-003-3 R6. The entity had a documented process of change control under CIP-003-3 R6, but failed to follow that process consistently. This noncompliance involves two instances.</p> <p>First, according to the entity's Enterprise Change Management process, change tickets must contain the explicit list of hosts (or assets) prior to the ticket being approved. The entity scheduled deployment of security patches to a series of 25 Critical Cyber Assets (a significant change) between August 12 and 13, 2015. When creating the change ticket, the analyst used a "parent group" available within the entity change management system to identify the group of assets intended to receive the security patch rather than the specific cyber assets. The analyst was unaware that parent groups did not internally identify assets as CIP Cyber Assets, causing the system to skip an automated validation step. For CIP Cyber Assets, there is an automated validation step where the change management system requires the analyst to assess and identify if the change activity is a significant change. As a result of using the parent group, the change management system did not flag the presence of CIP Cyber Assets being changed. This led to the analyst not identifying the intended change as significant, and thus not executing test procedures.</p> <p>The entity identified the issue shortly thereafter on August 25, 2015, through a control in its patch management process. As part of this process, a different analyst reviewed all patch management change tickets and attempted to obtain all post-test data. During this review, the analyst detected that the change was not identified as significant in the system, although it should have been. On August 27, 2015, the entity executed the test procedures and verified that no cyber security controls were adversely impact as a result of the change.</p> <p>Second, on October 16, 2015, a Security Analyst was assisting another employee with a change ticket submitted the day before to upgrade firmware on Critical Cyber Assets. The Security Analyst asked for more recent pre-change test procedures evidence than provided in the ticket. In response, the employee stated that they had already upgraded the firmware on the assets on October 12, 2015, without an approved [REDACTED] ticket, as required per the entity Enterprise Change Management Standard. The Security Analyst asked for new test procedures and confirmed the firmware had been updated prior to the submission of the change ticket. Upon discovery of the issue, the entity ran test procedures on the asset and determined that security controls were not impacted by the change.</p> <p>The root cause of this noncompliance was the responsible employees' lack of familiarity with the change management system. This contributing factor relates to the management practice of workforce management, which involves training, education, and awareness to employees.</p> <p>The first instance began on August 12, 2015, when the entity failed to appropriately test and validate changes to CIP Cyber Assets, and ended on August 27, 2015, when the entity executed the test procedures. The second instance began on October 12, 2015, when the firmware was upgraded, and ended on October 16, 2015, when the entity ran the test procedures.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. Applying patches or executing changes on CIP assets without properly executing test procedures could potentially introduce vulnerabilities. However, these risks were mitigated by the following factors. Regarding the first instance, the entity quickly detected the issue through its verification controls and thereafter quickly mitigated the issue. Regarding the second issue, the entity had been using similar cyber assets with updated software version installed through the entity's compliance validation processes with no impact to the BPS. Thus, it was unlikely (and later proven) that installing the same software version to the assets in question would not adversely affect the entity's system. ReliabilityFirst also notes that the entity also executed test procedures after the fact and determined that security controls were not affected by these changes. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because some of the prior noncompliance involve different root causes. For other prior noncompliance, while the current noncompliance involves conduct that is arguably similar to the previous noncompliance, the current noncompliance continues to qualify for compliance exception treatment as it involves high-frequency conduct for which the entity has demonstrated an ability to promptly identify and correct noncompliance. The entity has shown significant improvement from prior noncompliance to more current noncompliance with respect to very quickly identifying the noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed Test Procedures for all affected Cyber Assets; 2) performed refresher training to patch teams, on the entity's change management process to ensure they are aware of the process for entering change tickets for CIP Cyber Assets; and 3) modified the Change Control Review Process to ensure that only addressable cyber assets are included in change tickets via a review by the [REDACTED] and [REDACTED] analysts. The modification included training to the [REDACTED] and [REDACTED] on rejecting tickets without a cyber asset. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2016015835	CIP-003-3	R6			2/11/2016	5/24/2016	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On June 10, 2016, the entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-003-3 R6. In two instances, the entity failed to follow its change control process under CIP-003-3 R6.</p> <p>First, on February 10, 2016, a non-CIP portion of the entity's environment was upgraded. The next day, on February 11, 2016, the entity discovered that the backup process for the upgraded servers would not work after the upgrade. To rectify the issue as quickly as possible, the Database Administrators began to upgrade the backup software on all relevant servers without following the change management process. In the process, software on two CIP (Physical Access Control Systems (PACS)) servers was upgraded without following the process. The entity discovered the issue through its change control discovery tool on May 16, 2016.</p> <p>Second, on April 21, 2016, an analyst updated the entity's Virtual Private Network (VPN) infrastructure, used for remote access, to a new version. When users logged into the VPN from three CIP scoped (PACS) workstations, the VPN client processed the update automatically, applying updated software on the CIP workstations. As such, software on the workstations was updated without going through the CIP change management process. The entity discovered the issue through its change discovery tool on May 2, 2016.</p> <p>The root cause of the first instance was insufficient training regarding change management. For the second instance, the root cause was lack of awareness regarding the relationship between the VPN upgrade and related workstations. This noncompliance involve workforce management, which includes providing sufficient training to all responsible employees. This noncompliance also involves asset and configuration management, as the entity's processes lacked sufficient controls to manage the effects of implementing changes to assets.</p> <p>The entity verified that no security controls were impacted by the unauthorized changes.</p> <p>The first instance began on February 11, 2016, when the entity made changes without following its change control process, and ended May 24, 2016, when the entity completed the required scans. The second instance began April 21, 2016, when the entity made a change without following its change control process, and ended May 18, 2016, when the entity competed the required scans.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. Applying patches or executing changes on CIP assets without properly executing test procedures could potentially introduce vulnerabilities. However, these risks were mitigated by the following factors. In both instances, the entity self-identified the instances relatively quickly. In both instances, redundant cyber assets were available (i.e., the entity had redundant workstations and servers). The entity would have utilized these redundant cyber assets if the cyber assets on which the unauthorized system updates occurred were negatively affected. Moreover, if the redundant workstations failed, the entity has an additional spare workstation it would utilize (i.e., the entity also has a backup workstation for the redundant workstation). Additionally, if the changes had affected security controls (for example, opened unapproved ports), additional mitigations were in place on the cyber assets at issue, including blocking internet access at the firewall level and additional monitoring (e.g., IDS, anti-malware, physical, etc.). ReliabilityFirst also notes the entity also executed test procedures after the fact and determined that security controls were not affected by these changes. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because some of the prior noncompliance involve different root causes. For other prior noncompliance, while the current noncompliance involves conduct that is arguably similar to the previous noncompliance, the current noncompliance continues to qualify for compliance exception treatment as it involves high-frequency conduct for which the entity has demonstrated an ability to promptly identify and correct noncompliance. The entity has shown significant improvement from prior noncompliance to more current noncompliance with respect to very quickly identifying the noncompliance. Additionally, ReliabilityFirst notes that regarding the second instance, the entity's mitigation for the current noncompliance is much more robust than the prior noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) performed compliance scans to determine that no security controls were impacted by the changes; 2) developed a change management section that will be included within the corporate-wide annual CIP training to re-inforce the importance of following the published change management procedures; and 3) provided training to all applicable personnel. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017017324	CIP-010-2	R1	[REDACTED]	[REDACTED]	2/6/2017	5/31/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On March 22, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-010-2 R1. On February 6, 2017, an entity analyst launched a client application, [REDACTED], on an Electronic Access Control or Monitoring Systems (EACMS)-ID server. Upon start-up, the [REDACTED] client prompted the analyst to perform an upgrade. The analyst chose to perform the upgrade on the client at that time. This was an unauthorized change and detected on the following day, February 7, 2017, as a result of the entity's [REDACTED] scans against the server. Upon identifying the issue, the entity's IT Compliance team reviewed the reports on the security controls from before and after the change and determined that there was no impact to any security controls on the server as a result of the upgrade.</p> <p>The root causes were a failure to recognize the change as requiring change management steps, which involves the management practice of workforce management, as well as the lack of controls to identify the auto-update feature of the software.</p> <p>The noncompliance started on February 6, 2017, the date the entity was required to comply with CIP-010-2 R1 and ended on May 31, 2017, when the entity completed its Mitigation Plan.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The [REDACTED] client is an authorized piece of software for the server, and the software required the upgrade in order for the user to operate the application. This reduces the likelihood that the upgrade would cause security issues with the application. Additionally, a very small number of entity employees have access to [REDACTED], [REDACTED]. The entity also quickly detected the change and confirmed that the security controls were not adversely affected by the change. ReliabilityFirst also notes that the upgrade would have been applied later to the server through the entity's normal change management process in any event. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because some of the prior noncompliance involve different root causes. For other prior noncompliance, while the current noncompliance involves conduct that is arguably similar to the previous noncompliance, the current noncompliance continues to qualify for compliance exception treatment as it involves high-frequency conduct for which the entity has demonstrated an ability to promptly identify and correct noncompliance. The entity has shown significant improvement from prior noncompliance to more current noncompliance with respect to very quickly identifying the noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reviewed security controls for impact of unauthorized changes and took action for impacted controls if needed; 2) conducted training session with department staff. The training session included information on the entity's Change Management Process (including how a baseline is defined, and what types of changes would require change management). The session would also serve as a post-mortem on why the initial issue was a problem, which led the entity to self-report; and 3) removed the [REDACTED] client from all EACMS-ID cyber assets (as it is not possible to disable the auto-update feature). <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2016016354	CIP-005-5	R1	[REDACTED]	[REDACTED]	7/1/2016	9/9/2016	Audit	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED] ReliabilityFirst determined that [REDACTED] as a [REDACTED] and [REDACTED] was in violation of CIP-005-5 R1. ReliabilityFirst identified the violation during a Compliance Audit conducted from [REDACTED]. Seven of the entity's Bulk Electric System (BES) Cyber Systems that the entity identified as Protected Cyber Assets (PCA) were connected via a routable protocol to a network, but did not reside within a defined Electronic Security Perimeter (ESP) and network traffic to and from these BES Cyber Systems was not through an identified Electronic Access Point (EAP). These BES Cyber Systems bridged both ESP and non-ESP network segments. This occurred because a former ESP was declassified and these PCAs were overlooked during the decommissioning of the former ESP. As such, the entity continued to classify these systems as PCAs and the assets continued to be monitored and protected by [REDACTED]. Upon identification at audit, the entity exercised an emergency shutdown on all assets.</p> <p>The root cause was not following the entity's decommissioning process relating to the former ESP. This violation involves the management practice of asset and configuration management because the entity failed to manage the effects of implementing changes to assets.</p> <p>This noncompliance started on July 1, 2016, the date the entity was required to comply with CIP-005-5 R1 and ended on September 9, 2016, when the entity completed its emergency change control procedure and removed the devices.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The potential risk was the possibility of unwanted network traffic into the ESP. The risk here is mitigated because the entity continued to classify these assets as PCA and thus, except for CIP-005-5 R1, Parts 1.1 and 1.2, the assets were protected pursuant to the CIP Standards. For example, the assets continued to be monitored for baseline changes, met the password requirements, and had updated antivirus. Also, the assets were not directly accessible from the user network. [REDACTED] No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance involved different facts and circumstances and root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) sent an email to entity administrators requesting all interfaces to be shut down for the identified systems; 2) sent an email noting that the identified systems were offline; 3) created change control tickets to retire each of the identified cyber assets; and 4) updated the support ticket to indicate all servers were decommissioned and degaussed. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017017618	CIP-007-6	R2	[REDACTED]	[REDACTED]	12/7/2016	4/6/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On May 16, 2017, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-007-6 R2. On February 28, 2017, during a routine patch management evidence validation process, the entity identified one patch mitigation plan for a patch affecting four assets that was not extended within the specified timeframe. In response, the entity conducted an extent of condition review and identified 12 additional instances where the entity allowed mitigation plans to expire without implementing the patch or extending the mitigation plans. The 12 mitigation plans expired on February 23, 2017. The entity extended 11 of the mitigation plans on February 28, 2017 and the final Mitigation plan on March 7, 2017.</p> <p>Additionally, on April 6, 2017, the entity expanded the extent of condition and identified one patch mitigation plan for a patch on an asset that was not extended within the specified timeframe. The mitigation plan expired on December 7, 2016 and the entity extended the mitigation plan on April 6, 2017.</p> <p>Twelve instances related to four Electronic Access Control or Monitoring systems (EACMS) and one instance related to four Bulk Electric System Cyber Assets.</p> <p>The root cause of the possible violation was an insufficient patch management process. More specifically, the entity did not review all open CIP Version 5 patch mitigation target dates in weekly review meetings and instead only reviewed a subset based on analyst assigned instead of the date due. At the time of the CIP Version 5 transition, this weekly review meeting was already occurring, but was not documented at a granular level to instruct personnel on how to filter the list to perform the review.</p> <p>This noncompliance started on December 7, 2016, the earliest date a mitigation plan expired, and ended on April 6, 2017, when the entity extended that mitigation plan.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. For 12 of the 13 patches, the entity quickly identified and corrected the violation. More specifically, the entity extended most of the mitigation plans only five days after they expired and one mitigation plan two weeks after it expired. For the final patch, the entity extended the mitigation plan 4 months after it expired. However, for all mitigation plans, the security controls that mitigated the vulnerabilities were in place throughout the duration of the violation, thus reducing the risk that the assets could be compromised. Additionally, all patches were rated medium to low criticality. The entity generally implements the more critical patches within 35 days of assessing the patches and creates mitigation plans for only less critical patches. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because most of the prior noncompliance involved different facts and circumstances and root causes. Although one prior noncompliance is arguably similar to the current noncompliance, the current noncompliance continues to qualify for compliance exception treatment because it involved high frequency conduct, posed only minimal risk, and the entity quickly detected and corrected the noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) extended the mitigation plans as required by the entity's patch mitigation plan process; 2) reminded responsible personnel of the requirements of the documented entity's patch mitigation plan process, including the importance of following procedure and the impact of non-compliance; 3) updated and implemented its CIP Version 5 Mitigation Plan Extension Process to add steps: (a) review/update live system of record data in weekly meetings and (b) filter all patches by patch/mitigation due date; 4) performed full reconciliation of all patch mitigation plan dates from July 1, 2016 to the present. The entity confirmed that all mitigation dates were implemented within the timeframe specified or revised to extend the timeframe specified; and 5) enabled SharePoint features to generate mitigation plan extension plan process reminder and approval emails and track them centrally. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018652	CIP-007-6	R2			6/13/2017	8/7/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On November 7, 2017, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-007-6 R2. The entity did not meet the criteria laid out in CIP-007 R2 Part 2.3 for the [REDACTED] patch set [REDACTED]. The patch bundle was not installed, nor was a mitigation plan created within the required 35 days of the entity's evaluation of applicability.</p> <p>On May 8, 2017, the entity assessed a patch, determined that it was applicable to its system, and entered the patch details into the Patch Management Tracking SharePoint site. However, when entering the details into the site, the analyst failed to include the "applicability approved date," which prevented the automated notifications within SharePoint from alerting the security analysts of the deadline to install the patch or create a mitigation plan. The missing data was not added until June 18, 2017. The entity's security analysts were alerted to the missing mitigation plan on August 7, 2017 during the preparation for patch deployment. Once the security analysts were notified, they immediately (same day) created the mitigation plan. At that time, they determined that existing controls were already in place and sufficient to mitigate the vulnerability.</p> <p>The root causes of the possible violation was that that analyst failed to perform a quality inspection of the SharePoint entry as required by the entity's procedures and the process lacked a technical control to ensure the applicability approved date is entered in a timely manner. Accordingly, this possible violation involves the management practice of verification because the entity's verification controls were insufficient.</p> <p>This noncompliance started on June 13, 2017, the date by which the entity was required to install the patch or create a mitigation plan, and ended on August 7, 2017, when the entity created the mitigation plan.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. Although the entity was almost two month late in creating the mitigation plan, there was minimal risk to the bulk power system because the security controls required to reduce the risk of the open vulnerabilities were already in place on the impacted cyber assets. And, although there was not a formal mitigation plan in place, the entity documented that the patch was applicable and began the process of installing the patch before the noncompliance was even identified. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because most of the prior noncompliance involved different facts and circumstances and root causes. Although one prior noncompliance is arguably similar to the current noncompliance, the current noncompliance continues to qualify for compliance exception treatment because it involved high frequency conduct, posed only minimal risk, and the entity quickly detected and corrected the noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the required patch management mitigation plan documenting the controls in-place to reduce the severity of the security vulnerabilities; 2) used regularly scheduled patch management meeting to discuss potential technical control remedy; 3) implemented a technical control to require applicability approved date when entering data in the entity's patch management SharePoint site. Through this control, the date must be entered before the analyst can complete the patch data entry; 4) inspected other SharePoint entries from July 1, 2016 to ensure there are no others with missing applicability dates; and 5) trained the patch evaluation staff on the importance of following the procedure. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017017733	CIP-010-2	R2	██████████	██████████	7/1/2016	6/20/2017	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On June 5, 2017, ██████████ submitted a Self-Report to ReliabilityFirst stating that, as a ██████████ ██████████ and ██████████ it was in violation of CIP-010-2 R2. This violation involves two instances of a failure to monitor baselines. Both instances occurred because assets were added to the entity's baseline tool, ██████████, outside of the normal onboarding process, which circumvented the controls that the entity has in place to ensure baselines were being monitored.</p> <p>In the first instance, on December 8, 2016, the entity's ██████████ discovered that the firmware version on an ██████████ Electronic Access Control or Monitoring systems (EACMS) located at the entity's ██████████ datacenter had not been reviewed since before CIP version 5's effective date of July 1, 2016. The asset's associated scheduled firmware scan in the monitoring tool was directed to the asset's cluster counterpart at the entity's ██████████ datacenter. Therefore, the ██████████ cyber asset was being scanned twice, while the ██████████ cyber asset was not being scanned directly. Upon identifying the error, on December 9, 2016, the analyst immediately corrected the issue. Once scanned, the monitoring tool detected no changes since the baseline was originally taken in May 2016. Additionally, the ██████████ examined all similar cyber assets in ██████████ and found no other discrepancies.</p> <p>In the second instance, the recurring configuration monitoring task was not set up in ██████████ for four firewalls (EACMS) after their initial baselines were recorded. Baselines for two assets were initially created on January 3, 2017, and baselines for the remaining two assets were created on January 27, 2017. The issue was discovered on March 16, 2017, and resolved on March 20, 2017, which means the entity did not monitor baselines for these four assets for 48 days (and they were required to monitor baselines at least once every 35 calendar days). Once scanned, the monitoring tool detected no changes since the baseline was originally taken in January 2017. These four firewalls were added to ██████████ outside of the normal onboarding process to rectify a previously identified violation (RFC2017017371) and the monitoring task was not set up after manually capturing the initial baseline.</p> <p>Both issues were identified through a detective control. More specifically, the entity identified the issues during its quarterly comparison of what cyber assets are in ██████████ and the list of CIP-scoped Cyber Assets.</p> <p>The root cause of both instances was that the assets were added to the baseline monitoring tool outside of the normal onboarding process, which circumvented the controls that the entity has in place to ensure recurring monitoring is set up. To address this, the entity has implemented a new asset lifecycle management service that prohibits CIP-scoped assets from being classified as such without ensuring a baseline and the recurring monitoring task have been implemented.</p> <p>This noncompliance on started July 1, 2016, the date the entity was required to comply with CIP-010-2 R2 and ended on June 20, 2017, when the entity completed its Mitigation Plan.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The potential risk of not monitoring baselines is that it reduces the entity's ability to identify unauthorized activity, changes, or vulnerabilities. This risk was mitigated here based on the following factors. In all instances, the assets had all other required security protections (e.g., patching, monitoring, logging, and change control), thus reducing the potential that it would be compromised. Regarding the first instance (██████████ EACMS), given the nature of the specific type of asset and how it works with other similar assets in a cluster, any unauthorized change to the ██████████ cyber asset would have been detected by the other ██████████ cyber asset in the cluster, thus triggering an investigation and corrective actions. Regarding the second instance (██████████) the entity quickly identified and corrected the violation, thus reducing the amount of time that there was any increased risk to the system as a result of the violation. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the ██████████ cyber asset's record in ██████████ to reflect the correct IP address and enable the monitoring task for the firewall cyber assets in ██████████ 2) implemented a new asset lifecycle management service that prohibits EACMS (and other CIP scoped assets) from being classified as such without ensuring a baseline has been completed. (The service also ensures all other cyber security controls are in place.) The ██████████t service is implemented via the entity's ██████████ tool as an electronic workflow with gates that requires a successful implementation and confirmation of CIP cyber security controls prior to being used as a CIP scoped asset; and 3) trained the appropriate personnel on the update to the pre-production baseline inspection practices. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019573	CIP-011-2	R1	[REDACTED]	[REDACTED]	7/1/2016	6/5/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 13, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-011-2 R1. On January 30, 2018, the entity discovered that a substation and system protection print for a substation, which was not properly classified as Bulk Electric System Cyber System Information (BCSI), contained CIP protected information. The print was electronically housed in the non-CIP Information Repository (CIR) portion of the entity's [REDACTED] and physically housed in an [REDACTED] cabinet within the substation. Subsequently, the entity conducted an extent of condition review and identified 11 more prints showing similar information that were not properly classified as BCSI.</p> <p>The root cause of this noncompliance was the fact that these prints were not included within the sample set of prints the entity evaluated during preparations for CIP-011-2 implementation. This major contributing factor involves the management practice of information management, which includes protecting information items and managing information item confidentiality and privacy.</p> <p>This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-011-2 R1 and ended on June 5, 2018, when the entity corrected the drawings and disposed of the old drawings.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. First, the drawings at issue only showed how certain BCAs were connected to each other, not how to actually connect to them remotely. Therefore, potential malicious use of this information would require someone to either bypass the entity's physical security controls and gain physical access to the substation or bypass the entity's electronic security controls for remote access. Second, potential unauthorized access to the electronic copies of the prints was limited to 40 entity personnel and approved contractors, who are trusted personnel. These 40 users had access to the non-CIR portion of the [REDACTED] where the prints were being stored, but not to the CIR portion where they should have been stored. Additionally, the locked cabinets in which the physical copies of the prints were stored are accessible only by authorized protection and control technicians. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance were the result of different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the BCSI from the twelve drawings. The entity created twelve new drawings and the BCSI was placed on these drawings and labeled as CIP Protected; 2) provided training to entity [REDACTED] team on investigation results and proper handling of elementary wiring diagrams; 3) issued work orders to remove all twelve drawings with BCSI from substation drawing cabinets and replaced them with non-BCSI drawings; and 4) collected and disposed of the hard copies of the twelve drawings by cross-cut shredding. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018543	CIP-010-2	R1	████████████████████	██████████	7/1/2016	10/17/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 20, 2017, █████ submitted a Self-Report stating that, as a █████, it was in noncompliance with CIP-010-2 R1. On August 10, 2017, during the review of the 2017 Cyber Vulnerability Assessment (CVA), the entity discovered discrepancies between the firmware ID information captured within the █████ and the evidence collected for three Bulk Electric System Cyber Assets (BCAs) classified as medium impact without external routable connectivity (ERC). These three devices had an older version of the firmware installed in the field than what was listed in █████. Subsequently, the entity identified eight more BCAs classified as medium impact without ERC that had an older firmware version listed in █████, though they were updated in the field.</p> <p>The root cause of this noncompliance was the responsible individuals' failure to follow established procedure. For the initial three instances, the responsible individual failed to restart the devices after installing the new firmware, which prevented the changes from taking effect. For the latter eight instances, the relay technicians failed to thoroughly verify the firmware ID on the device against the information in █████. This major contributing factor involves the management practices of asset and configuration management, which includes controlling changes to assets and configuration items and baselines, verification, in that the entity failed to verify the field settings matched what was in █████, and workforce management, which includes managing the system to minimize human performance issues.</p> <p>This noncompliance started on July 1, 2016, because the issues with the latter eight relays existed prior to the effective date of CIP Version 5, and ended on October 17, 2017, when the entity corrected the issues with the initial 3 devices.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. First, this issue was limited to 11 out of 476 devices, which indicates that this was an isolated issue. Second, these devices do not have ERC. Therefore, potential malicious use would require physical access to the substation, which is controlled by █████ Physical Security Plan. Third, the updates associated with the firmware update that failed to install on the initial three relays did not provide any additional, or remove an existing, capability that would fall under NERC CIP scope. Fourth, for the latter eight relays, they were functioning properly and up-to-date in the field, so the issue was documentation-related. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance were either the result of different causes or involve conduct that ReliabilityFirst determined constitutes high frequency conduct that does not warrant an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the baseline information of all impacted devices in █████ accordingly; 2) provided refresher training on existing CVA/Security Controls Verification (SCV) procedure document to Relay Techs, re-emphasizing the need to perform a thorough comparison of firmware and other pertinent baseline information, requirement to notify the CIP Team when mismatches are discovered and utilizing device instruction manuals as necessary with guidance on where to locate the manuals; 3) created setting requests and a Work Order to install the latest security patches for these three (3) BCAs, and also made sure they are reset after the installation; 4) updated the existing Pre-Execution, SCV & CIP Post-Execution Review Process document to include what the SCV approver needs to verify prior to approving SCV forms in █████; and 5) created a CVA Job Process document that lists and explains what the Sr. Engineering Tech Specialist or designee should look for during the CVA activity review prior to approving the CVA forms in █████, and training provided on the document to identified/prospective users. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018542	CIP-010-2	R1	[REDACTED]	[REDACTED]	8/4/2017	8/4/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 20, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. On May 25, 2017, an individual in entity [REDACTED] performed an Authorized Change Request to upgrade commercially available backup software on 53 energy management system (EMS) workstations. However, that individual mistakenly omitted five devices that should have been included in the change ticket for the same work and installation. Subsequently, after that change request was closed out, a member of the [REDACTED] team realized, while reviewing backup logs for EMS workstations, that the five devices did not have the most current version of backup software.</p> <p>Consequently, on August 4, 2017, the entity upgraded the backup software on the remaining 5 EMS workstations. However, that upgrade was performed without submitting a new Authorized Change Request. The responsible individual mistakenly believed that a new change request was not needed because these 5 devices were supposed to be a part of the original upgrade. The entity identified this error 6 days later while performing routine baseline monitoring, which is designed to catch these types of errors.</p> <p>The root cause of this noncompliance was the responsible individual's mistaken belief that a new change request was not necessary. This major contributing factor involves the management practice of workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on August 4, 2017, when the entity upgraded the software on the 5 devices without a new change request and ended later that day when the entity completed the change and updated documentation to reflect the change.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. First, these 5 devices were supposed to have been a part of the original upgrade change ticket. So, the change was tested and not expected to have any adverse impact on the devices. Second, the entity identified the issue quickly through its normally occurring internal controls. Third, these devices had local redundancy as well as off-site backup. Had there been an issue, the operators could have moved to other consoles in the environment to continue their work. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance are either the result of different causes or involve conduct that ReliabilityFirst determined constitutes high frequency conduct that does not warrant an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) conducted an investigation into the incident with [REDACTED], [REDACTED], and [REDACTED] to determine if a cybersecurity incident occurred; 2) held a meeting with the performer on August 11, 2017 to reinforce the [REDACTED] CIP-010 R1.2 change management procedure; 3) re-trained the ticket performer on the components of a device baseline and the importance of fully assessing a potential impact to that device baseline when completing changes; and 4) conducted training with [REDACTED] personnel on [REDACTED] tool and compliance change management requirements. This includes acquiring baseline change approvals prior to work. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018477	CIP-007-3a	R5	[REDACTED]	[REDACTED]	4/30/2015	11/16/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 6, 2017, [REDACTED], as a [REDACTED], submitted a Self-Report to ReliabilityFirst stating that it was in noncompliance with CIP-007-3a R5. On July 10, 2017, [REDACTED] determined that two previously unknown default accounts associated with [REDACTED] assets were not identified or inventoried. Because these default accounts were not identified or inventoried, the [REDACTED] failed to identify those individuals with access to these accounts.</p> <p>The root cause of this noncompliance were: (a) the vendor failed to identify these accounts in its documentation; and, (b) the [REDACTED] failed to realize when the vendor corrected this error and updated its documentation. As to the first issue, these accounts were not previously identified in vendor documentation of accounts on the assets, and the configuration rule sets released by the vendor were not coded to identify these accounts either. The default accounts are associated with the [REDACTED] application integrated into each of the [REDACTED] assets. The accounts existed when the assets were placed into production before CIP Version 5 became effective. With respect to the second issue, the vendor updated its documentation for versions [REDACTED] and [REDACTED] on November 7, 2016, to include references to the two previously unknown default accounts. These changes were noted in the document version control, but no other notification was issued. As a result, the [REDACTED] failed to identify the update.</p> <p>This noncompliance started on April 30, 2015, when the [REDACTED] activated the accounts and ended on November 16, 2017, when the [REDACTED] ensured that all accounts were properly identified and inventoried.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. First, the default accounts, though previously unknown, are embedded into already protected assets behind several layers of physical and logical security. Second, the accounts are isolated from remote access except to authenticated administrators, all of whom are approved for administrative access to the assets. And all of these individuals are trusted and authorized [REDACTED] administrators with up-to-date NERC CIP Training and Personnel Risk Assessments. Third, the same potential population of users who would have access are the same individuals that will continue to have access as authorized administrators. And lastly, aside from these authorized administrators, remote access is restricted to the device and the accounts. No other individuals had potential access to the accounts in question. The issue is limited to documentation and tracking at [REDACTED] of the accounts. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the [REDACTED]' compliance history should not serve as a basis for applying a penalty because they either arose from different causes or constitute high frequency conduct that ReliabilityFirst determined did not warrant an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) conducted Stand-down meetings with all affected [REDACTED] teams to reinforce the need to review vendor materials or contact vendor to identify changes to shared accounts and security controls and not simply relying on [REDACTED] to identify changes; 2) updated [REDACTED] to include [REDACTED] and [REDACTED] accounts for each area of responsibility: [REDACTED], [REDACTED] and [REDACTED]; 3) compared Shared Accounts from [REDACTED] environments to the current [REDACTED]. The [REDACTED] also verified the accounts are accounted for and are represented in a consistent manner. Updated Inventory as necessary. Provided resultant [REDACTED] report of all [REDACTED] Shared Accounts to [REDACTED] performer via email; [REDACTED] performer must acknowledge receipt of report; 4) updated [REDACTED] with the [REDACTED] Shared Accounts [REDACTED] and [REDACTED]. Also updated the roles that will authorize access and administer these accounts for each area of responsibility: [REDACTED], [REDACTED] and [REDACTED]; 5) compared consolidated list of Shared Accounts from [REDACTED] to the Current Shared Accounts in [REDACTED]. The [REDACTED] verified all accounts are accounted for and are represented in a consistent manner; 6) developed and delivered awareness material to reinforce the need to review documentation or contact the vendor to identify for any system with potential changes to Shared Accounts and Security Controls. Target audience is Key technical performers, Compliance Teams, Business Unit Compliance Contacts, Enterprise Standard Owners, and Legal; and 7) identified and updated existing, or created new, CIP-007 Systems Security Management documentation to provide guidance needed to help ensure that Shared Accounts and Security Controls are being identified and addressed for new installations and updates to Bulk Electric System Cyber Assets. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018478	CIP-007-3a	R5	[REDACTED]	[REDACTED]	4/30/2015	11/16/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 6, 2017, [REDACTED], as a [REDACTED] r, submitted a Self-Report to ReliabilityFirst stating that it was in noncompliance with CIP-007-3a R5. On July 10, 2017, [REDACTED] determined that two previously unknown default accounts associated with [REDACTED] assets were not identified or inventoried. Because these default accounts were not identified or inventoried, the [REDACTED] failed to identify those individuals with access to these accounts.</p> <p>The root cause of this noncompliance were: (a) the vendor failed to identify these accounts in its documentation; and, (b) the [REDACTED] failed to realize when the vendor corrected this error and updated its documentation. As to the first issue, these accounts were not previously identified in vendor documentation of accounts on the assets, and the configuration rule sets released by the vendor were not coded to identify these accounts either. The default accounts are associated with the [REDACTED] application integrated into each of the [REDACTED] assets. The accounts existed when the assets were placed into production before CIP Version 5 became effective. With respect to the second issue, the vendor updated its documentation for versions [REDACTED] and [REDACTED] on November 7, 2016, to include references to the two previously unknown default accounts. These changes were noted in the document version control, but no other notification was issued. As a result, the [REDACTED] failed to identify the update.</p> <p>This noncompliance started on April 30, 2015, when the [REDACTED] activated the accounts and ended on November 16, 2017, when the [REDACTED] ensured that all accounts were properly identified and inventoried.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. First, the default accounts, though previously unknown, are embedded into already protected assets behind several layers of physical and logical security. Second, the accounts are isolated from remote access except to authenticated administrators, all of whom are approved for administrative access to the assets. And all of these individuals are trusted and authorized [REDACTED] administrators with up-to-date NERC CIP Training and Personnel Risk Assessments. Third, the same potential population of users who would have access are the same individuals that will continue to have access as authorized administrators. And lastly, aside from these authorized administrators, remote access is restricted to the device and the accounts. No other individuals had potential access to the accounts in question. The issue is limited to documentation and tracking at [REDACTED] of the accounts. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the [REDACTED]' compliance history should not serve as a basis for applying a penalty because they either arose from different causes or constitute high frequency conduct that ReliabilityFirst determined did not warrant an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) conducted Stand-down meetings with all affected [REDACTED] teams to reinforce the need to review vendor materials or contact vendor to identify changes to shared accounts and security controls and not simply relying on [REDACTED] to identify changes; 2) updated [REDACTED] to include [REDACTED] and [REDACTED] accounts for each area of responsibility: [REDACTED], [REDACTED] and [REDACTED] 3) compared Shared Accounts from [REDACTED] environments to the current [REDACTED]. The [REDACTED] also verified the accounts are accounted for and are represented in a consistent manner. Updated Inventory as necessary. Provided resultant [REDACTED] report of all [REDACTED] Shared Accounts to [REDACTED] performer via email; [REDACTED] performer must acknowledge receipt of report; 4) updated [REDACTED] with the [REDACTED] Shared Accounts [REDACTED] and [REDACTED] Also updated the roles that will authorize access and administer these accounts for each area of responsibility: [REDACTED], [REDACTED] and [REDACTED] 5) compared consolidated list of Shared Accounts from [REDACTED] to the Current Shared Accounts in [REDACTED]. The [REDACTED] verified all accounts are accounted for and are represented in a consistent manner; 6) developed and delivered awareness material to reinforce the need to review documentation or contact the vendor to identify for any system with potential changes to Shared Accounts and Security Controls. Target audience is Key technical performers, Compliance Teams, Business Unit Compliance Contacts, Enterprise Standard Owners, and Legal; and 7) identified and updated existing, or created new, CIP-007 Systems Security Management documentation to provide guidance needed to help ensure that Shared Accounts and Security Controls are being identified and addressed for new installations and updates to Bulk Electric System Cyber Assets. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018479	CIP-007-3a	R5	[REDACTED]	[REDACTED]	4/30/2015	11/16/2017	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On October 6, 2017, [REDACTED], as a [REDACTED], submitted a Self-Report to ReliabilityFirst stating that it was in noncompliance with CIP-007-3a R5. On July 10, 2017, [REDACTED] determined that two previously unknown default accounts associated with [REDACTED] assets were not identified or inventoried. Because these default accounts were not identified or inventoried, the [REDACTED] failed to identify those individuals with access to these accounts.</p> <p>The root cause of this noncompliance were: (a) the vendor failed to identify these accounts in its documentation; and, (b) the [REDACTED] failed to realize when the vendor corrected this error and updated its documentation. As to the first issue, these accounts were not previously identified in vendor documentation of accounts on the assets, and the configuration rule sets released by the vendor were not coded to identify these accounts either. The default accounts are associated with the [REDACTED] application integrated into each of the [REDACTED] assets. The accounts existed when the assets were placed into production before CIP Version 5 became effective. With respect to the second issue, the vendor updated its documentation for versions [REDACTED] and [REDACTED] on November 7, 2016, to include references to the two previously unknown default accounts. These changes were noted in the document version control, but no other notification was issued. As a result, the [REDACTED] failed to identify the update.</p> <p>This noncompliance started on April 30, 2015, when the [REDACTED] activated the accounts and ended on November 16, 2017, when the [REDACTED] ensured that all accounts were properly identified and inventoried.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. First, the default accounts, though previously unknown, are embedded into already protected assets behind several layers of physical and logical security. Second, the accounts are isolated from remote access except to authenticated administrators, all of whom are approved for administrative access to the assets. And all of these individuals are trusted and authorized [REDACTED] administrators with up-to-date NERC CIP Training and Personnel Risk Assessments. Third, the same potential population of users who would have access are the same individuals that will continue to have access as authorized administrators. And lastly, aside from these authorized administrators, remote access is restricted to the device and the accounts. No other individuals had potential access to the accounts in question. The issue is limited to documentation and tracking at [REDACTED] of the accounts. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the [REDACTED]' compliance history should not serve as a basis for applying a penalty because they either arose from different causes or constitute high frequency conduct that ReliabilityFirst determined did not warrant an alternative disposition method.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) conducted Stand-down meetings with all affected [REDACTED] teams to reinforce the need to review vendor materials or contact vendor to identify changes to shared accounts and security controls and not simply relying on [REDACTED] to identify changes; 2) updated [REDACTED] to include [REDACTED] and [REDACTED] accounts for each area of responsibility: [REDACTED], [REDACTED] and [REDACTED] 3) compared Shared Accounts from [REDACTED] environments to the current [REDACTED]. The [REDACTED] also verified the accounts are accounted for and are represented in a consistent manner. Updated Inventory as necessary. Provided resultant [REDACTED] report of all [REDACTED] Shared Accounts to [REDACTED] performer via email; [REDACTED] performer must acknowledge receipt of report; 4) updated [REDACTED] with the [REDACTED] Shared Accounts [REDACTED] and [REDACTED]. Also updated the roles that will authorize access and administer these accounts for each area of responsibility: [REDACTED], [REDACTED] and [REDACTED] 5) compared consolidated list of Shared Accounts from [REDACTED] to the Current Shared Accounts in [REDACTED]. The [REDACTED] verified all accounts are accounted for and are represented in a consistent manner; 6) developed and delivered awareness material to reinforce the need to review documentation or contact the vendor to identify for any system with potential changes to Shared Accounts and Security Controls. Target audience is Key technical performers, Compliance Teams, Business Unit Compliance Contacts, Enterprise Standard Owners, and Legal; and 7) identified and updated existing, or created new, CIP-007 Systems Security Management documentation to provide guidance needed to help ensure that Shared Accounts and Security Controls are being identified and addressed for new installations and updates to Bulk Electric System Cyber Assets. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018480	CIP-007-3a	R5	[REDACTED]	[REDACTED]	4/30/2015	11/16/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 6, 2017, [REDACTED] as a [REDACTED], submitted a Self-Report to ReliabilityFirst stating that it was in noncompliance with CIP-007-3a R5. On July 10, 2017, [REDACTED] determined that two previously unknown default accounts associated with [REDACTED] assets were not identified or inventoried. Because these default accounts were not identified or inventoried, the [REDACTED] failed to identify those individuals with access to these accounts.</p> <p>The root cause of this noncompliance were: (a) the vendor failed to identify these accounts in its documentation; and, (b) the [REDACTED] failed to realize when the vendor corrected this error and updated its documentation. As to the first issue, these accounts were not previously identified in vendor documentation of accounts on the assets, and the configuration rule sets released by the vendor were not coded to identify these accounts either. The default accounts are associated with the [REDACTED] application integrated into each of the [REDACTED] assets. The accounts existed when the assets were placed into production before CIP Version 5 became effective. With respect to the second issue, the vendor updated its documentation for versions [REDACTED] and [REDACTED] on November 7, 2016, to include references to the two previously unknown default accounts. These changes were noted in the document version control, but no other notification was issued. As a result, the [REDACTED] failed to identify the update.</p> <p>This noncompliance started on April 30, 2015, when the [REDACTED] activated the accounts and ended on November 16, 2017, when the [REDACTED] ensured that all accounts were properly identified and inventoried.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. First, the default accounts, though previously unknown, are embedded into already protected assets behind several layers of physical and logical security. Second, the accounts are isolated from remote access except to authenticated administrators, all of whom are approved for administrative access to the assets. And all of these individuals are trusted and authorized [REDACTED] administrators with up-to-date NERC CIP Training and Personnel Risk Assessments. Third, the same potential population of users who would have access are the same individuals that will continue to have access as authorized administrators. And lastly, aside from these authorized administrators, remote access is restricted to the device and the accounts. No other individuals had potential access to the accounts in question. The issue is limited to documentation and tracking at [REDACTED] of the accounts. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the [REDACTED]' compliance history should not serve as a basis for applying a penalty because they either arose from different causes or constitute high frequency conduct that ReliabilityFirst determined did not warrant an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) conducted Stand-down meetings with all affected [REDACTED] teams to reinforce the need to review vendor materials or contact vendor to identify changes to shared accounts and security controls and not simply relying on [REDACTED] to identify changes; 2) updated [REDACTED] to include [REDACTED] and [REDACTED] accounts for each area of responsibility: [REDACTED], [REDACTED] and [REDACTED]; 3) compared Shared Accounts from [REDACTED] environments to the current [REDACTED]. The [REDACTED] also verified the accounts are accounted for and are represented in a consistent manner. Updated Inventory as necessary. Provided resultant [REDACTED] report of all [REDACTED] Shared Accounts to [REDACTED] performer via email; [REDACTED] performer must acknowledge receipt of report; 4) updated [REDACTED] with the [REDACTED] Shared Accounts [REDACTED] and [REDACTED]. Also updated the roles that will authorize access and administer these accounts for each area of responsibility: [REDACTED] and [REDACTED]; 5) compared consolidated list of Shared Accounts from [REDACTED] to the Current Shared Accounts in [REDACTED]. The [REDACTED] verified all accounts are accounted for and are represented in a consistent manner; 6) developed and delivered awareness material to reinforce the need to review documentation or contact the vendor to identify for any system with potential changes to Shared Accounts and Security Controls. Target audience is Key technical performers, Compliance Teams, Business Unit Compliance Contacts, Enterprise Standard Owners, and Legal; and 7) identified and updated existing, or created new, CIP-007 Systems Security Management documentation to provide guidance needed to help ensure that Shared Accounts and Security Controls are being identified and addressed for new installations and updates to Bulk Electric System Cyber Assets. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019650	CIP-010-2	R3	[REDACTED]	[REDACTED]	7/1/2016	5/10/2018	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On April 26, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R3. On March 7, 2018, the entity completed its review of CIP-002 [REDACTED] devices in the [REDACTED] and identified one [REDACTED] that was not included on the [REDACTED] device list. As a result, the device had not been properly accounted for in the [REDACTED] and [REDACTED] and it did not receive a Cyber Vulnerability Assessment (CVA) in calendar years 2016 and 2017. [REDACTED]</p> <p>[REDACTED] The entity performed an extent of condition review and determined that this [REDACTED] was the only device affected out of 40 similar devices identified as [REDACTED].</p> <p>The root cause of this noncompliance was the responsible individual's failure to properly assess and flag this [REDACTED] device as [REDACTED] in [REDACTED]. This major contributing factor involves the management practice of workforce management, which includes managing the system to minimize human performance issues.</p> <p>This noncompliance started on July 1, 2016, when the entity should have properly identified, assessed, and performed a CVA for this [REDACTED] device, and ended on May 10, 2018, when the entity completed the CVA of this [REDACTED] device.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk associated with failing to perform a CVA for this [REDACTED] device is that the entity may miss a new or emerging threat to the security of the device. This risk was mitigated in this case by the following factors. First, this [REDACTED] device was the only one out of 40 similar devices that not properly identified and flagged as [REDACTED]. This fact demonstrates that this was an isolated issue and not indicative of a programmatic failure. Second, this device provides encrypted electronic [REDACTED], does not have External Routable Connectivity (ERC), cannot be accessed remotely, and is serially connected to [REDACTED], the remote access connection interface. [REDACTED] Accordingly, potential misuse of this device would require physical access to the site, which is protected per [REDACTED] Physical Security plan as a Medium Impact Bulk Electric System (BES) Cyber System without ERC. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior issues were the result of different causes.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) assessed affected [REDACTED] as a Medium Impact in [REDACTED], and flagged as Medium Impact in [REDACTED]; 2) conducted and approved Cyber Vulnerability Assessment on affected EACMS; and 3) conducted a refresher training on [REDACTED] for entity [REDACTED] personnel responsible for performing and approving Cyber Asset assessment. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019381	CIP-007-6	R2	[REDACTED]	[REDACTED]	11/3/2016	9/27/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On March 2, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2. On October 23, 2017, the entity discovered a near-miss scenario where a monthly patch source review (PSR) had not been automatically initiated for a set of recently installed Medium Impact Bulk Electric System Cyber Assets (BCAs) to fulfill the 35-calendar day review requirement. This scenario was a near-miss because the entity identified the problem within the 35-day period after the devices were installed, which allowed the entity to perform manual patch source reviews on the devices in [REDACTED] to maintain compliance. The entity determined that this situation was caused by a timing issue between when new devices are populated in [REDACTED] and when the systems lock down for patch discovery. Specifically, post-installation entry of new device attributes into the entity's [REDACTED] [REDACTED] has the potential to occur after [REDACTED] is locked for new entries and updates due to initiation of the monthly patch source review, which introduces the potential to miss the initial 35-day period for patch discovery.</p> <p>Based on this analysis of the near-miss scenario, the entity performed an extent of condition review of 110 new Medium Impact BCA installations since the July 1, 2016 effective date. The entity identified 5 Medium Impact BCAs for which the initial 35-day patch discovery period had been exceeded. Two BCAs (i.e., BCA [REDACTED] and BCA [REDACTED]) had their [REDACTED] performed during the next automatically scheduled review period. The other three BCAs had longer durations because the associated device and setting request statuses were not captured correctly in [REDACTED]. Therefore, [REDACTED] was not updated with the information to trigger a patch source review until the later date when the device and setting request statuses were updated in [REDACTED].</p> <p>The root cause of this noncompliance was a timing issue between when new devices are populated in [REDACTED] and when the systems lock down for patch discovery. Specifically, these 5 BCAs had their information entered into [REDACTED] after the patch source review system was locked for that period. This major contributing factor involves the management practices of asset and configuration management, which includes controlling changes to assets and configuration items and baselines, and implementation, because the issue involves the installation of new or modified devices.</p> <p>This noncompliance started on November 3, 2016, when the first 35-day window expired, and ended on September 27, 2017, when the entity completed all the patch source reviews for affected BCAs.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. First, the entity self-identified this issue by detecting and analyzing a near-miss scenario. This type of conduct demonstrates a commitment to ensuring the reliability, resiliency, and security of the BPS. Second, this issue was limited in scope, occurring on 5 out of 110 BCAs. Third, the five affected BCAs are not connected with any External Routable Connectivity, having only serial connections to Supervisory Control and Data Acquisition (SCADA) and [REDACTED] remote access connection interface). Consequently, malicious activity associated with these BCAs would require physical access to the substation, which is controlled according to [REDACTED] Physical Security Plan, which includes card readers and electronic keys. ReliabilityFirst also notes that no patches were released by the vendor during the time-lapse from when the devices went into service and when the patch source review was completed. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance either arose from different causes or involved conduct that ReliabilityFirst determined constitutes high frequency conduct that does not warrant an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) created an interim addendum to existing entity process document to generate ad-hoc patch source reviews once [REDACTED] is complete. This process will ensure that firmware ID and operating system information for newly installed entity [REDACTED] devices are populated in [REDACTED] for patch discovery activities, until a permanent technical solution is in place; 2) developed a script so that firmware ID and operating system information for pre-production devices in [REDACTED] are populated in the [REDACTED] NERC [REDACTED]; 3) modified [REDACTED] so that firmware ID and operating system information for pre-production devices are populated from [REDACTED] thereby ensuring that pre-production device information is available for initial patch source review while devices are still in pre-production status; 4) implemented functionality in [REDACTED] to perform PSRs on devices in pre-production status, ensuring that pre-production device baselines are accurate; and 5) will rescind interim process to generate ad-hoc PSRs once the permanent technical solution is in place. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018863	CIP-007-6	R3	[REDACTED]	[REDACTED]	10/13/2017	10/17/2017	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On December 15, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R3. On October 13, 2017, a production [REDACTED]</p> <p>The following Monday, the [REDACTED] discovered the issue while performing the weekly signature update monitoring process. The next day, the [REDACTED] was removed from maintenance and put into the production folder with the correct signature update policy applied.</p> <p>The root cause of this noncompliance was the fact that the responsible individual forgot to return the device to the production folder. This person did not have a guidance document to help ensure the device was returned to production. This major contributing factor involves the management practice of workforce management, which includes managing a system to minimize human performance issues.</p> <p>This noncompliance started on October 13, 2017, when the entity placed the device into maintenance mode and ended on October 17, 2017, when the entity placed the device back into production mode.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk associated with this noncompliance is that applying untested anti-virus signatures could cause degraded performance or failure of the [REDACTED]. This risk was mitigated in this case by the following factors. First, although the entity failed to test these anti-virus signatures, the vendor extensively tested them prior to deployment, which reduces the likelihood that they would have had an adverse impact on the device. Second, the entity had redundancy in the [REDACTED] to maintain logging and alerting if the device had become unavailable. Third, the entity quickly identified and corrected the noncompliance. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance arose from a different cause.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the [REDACTED] from maintenance mode and put into the production folder with the correct policy applied; 2) removed untested signatures from impacted Cyber Asset and deployed tested signatures; 3) placed the Production policy on the maintenance folder so that Production policies and tested signatures will be forced there; 4) created a job-aid describing the process, roles and responsibilities of placing [REDACTED] into maintenance mode; 5) developed training material for asset owners regarding the [REDACTED] maintenance mode job-aid process; and 6) provided training to Asset Owners. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018711	CIP-006-6	R2	[REDACTED]	[REDACTED]	9/1/2017	9/1/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On November 17, 2017, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R2. On September 1, 2017, the entity experienced issues with its visitor control program involving work being performed within a Physical Security Perimeter (PSP) by four individuals: two contractors and two subcontractors. Both contractors had valid Personnel Risk Assessments (PRAs) and NERC training, and both had previously performed work in other PSPs. However, only one of the contractors had authorized unescorted physical access rights to the particular PSP at issue in this case. (These individuals were working on the Computer Room Air Conditioning System, with no impact to the bulk power system.) But these contractors mistakenly believed that they both had authorized access to this PSP.</p> <p>When these four individuals entered the PSP, the contractor with authorized access badged in, and the other contractor tailgated behind without badging in and without logging his entry. Furthermore, at one point, the authorized contractor left the PSP, which left the unauthorized contractor and the two subcontractors in the PSP by themselves without an escort. Fifteen minutes later, when these three individuals left the PSP, a forced open alarm was received by the [REDACTED] Operations Center ([REDACTED] OC). These facts constitute two instances of noncompliance. First, the unauthorized contractor's tailgating into the PSP without logging in as a visitor. Second, the failure to continuously escort the unauthorized individuals within the PSP.</p> <p>The root cause of this noncompliance was the misbelief that both contractors had authorized unescorted access rights to the PSP at issue. This major contributing factor involves the management practice of workforce management, which includes controlling employees' access to assets.</p> <p>This noncompliance started on September 1, 2017, when the unauthorized contractor tailgated into the PSP without properly logging in, and ended on the same day when to the three unauthorized individuals exited the PSP.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. First, all of these individuals only had limited access to the locked server cabinets because they lacked credentials to electronically access any NERC equipment. Second, these individuals were working on the Computer Room Air Conditioning system, with no impact to the BPS. Third, even though he did not have authorized unescorted physical access rights to this particular PSP, the unauthorized contractor was trusted by the entity because he had a work history with the entity. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance were either the results of different causes or involve conduct that ReliabilityFirst has determined constitutes high frequency conduct that does not warrant an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) met with facilities vendor to provide reinforcement regarding access and escort duties in PSPs; 2) conducted a stand down within the facilities department to review NERC physical secure perimeter processes and continuous escort duties and expectations for proper visitor escorting to NERC PSPs; 3) worked with leadership to develop consistent leadership reinforcement materials; 4) modified the [REDACTED] to include required PSP access procedures and review with key staff; and 5) worked with leadership to roll out the communication to entity personnel with PSP access. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019841	CIP-004-6	R4	[REDACTED]	[REDACTED]	7/17/2017	3/14/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On June 5, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R4. On July 17, 2017, the entity granted a Corporate Security contractor access through its [REDACTED] system. The intended permission stated in the [REDACTED] ticket was [REDACTED]. The entity, however, incorrectly granted the following permission [REDACTED]. The entity discovered this issue during its Q1 2018 electronic access review.</p> <p>The Corporate Security contractor had all the necessary credentials (valid Personnel Risk Assessment (PRA) and up-to-date CIP training) to receive the greater permission (i.e. the unintended and unauthorized access).</p> <p>Regarding the root cause, the similarity in the two permission names contributed to the wrong permission being assigned to the Corporate Security contractor. Additionally, the entity did not have an effective control in place to validate and verify that correct access permissions were being assigned. Accordingly, this noncompliance involves the management practices of validation and verification.</p> <p>This noncompliance started on July 17, 2017, when the entity granted unauthorized access to the Corporate Security contractor, and ended on March 14, 2018, when the entity revoked the Corporate Security contractor's unauthorized access.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is allowing an unauthorized individual to access Bulk Electric System (BES) Cyber Systems, which could lead to the intentional compromise or misuse of BES Cyber Systems. The risk is minimized because the Corporate Security contractor had all the necessary credentials (valid PRA and up-to-date CIP training) to receive the unauthorized access. Additionally, the Corporate Security contractor is a trusted contractor who maintained many other physical and cyber access permissions with the entity. Lastly, ReliabilityFirst notes that the entity confirmed that the Corporate Security contractor never attempted to use the unauthorized access permission.</p> <p>No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance either arose from different root causes or constitute high frequency conduct that ReliabilityFirst determined did not warrant an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the [REDACTED] application to reflect the original [REDACTED] ticket access requested and revoked the Corporate Security contractor's unauthorized access; 2) verbally counseled the employee that granted the incorrect access. The employee later signed an attestation acknowledging that he had been verbally counseled; 3) renamed one of the two similar group names so they look different; and 4) implemented a change log where all changes are flagged and reviewed (typically next business day). <p>The new automated change log review will help ensure that the approved procedures and processes are being followed in the future. Additionally, as a detective measure, the entity routinely performs reviews of access changes using [REDACTED] automated reports and by conducting quarterly reviews.</p> <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019405	CIP-002-5.1a	R2	[REDACTED]	[REDACTED]	9/1/2017	1/31/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On March 12, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-002-5.1a R2. On January 30, 2018, during an independent compliance review of its NERC program, the entity discovered that it failed to timely review and approve its identification of Bulk Electric System (BES) Cyber Systems (BCS) and associated Cyber Assets in accordance with the Standard. Specifically, although the entity timely reviewed its BCS list, the entity's CIP Senior Manager did not approve the BCS list within 15 calendar months.</p> <p>The root cause of this noncompliance involved personnel issues, including the lack of backup personnel, within the group that administers the NERC compliance program at the entity. This major contributing factor involves the management practice of workforce management, which includes managing staff performance.</p> <p>This noncompliance started on September 1, 2017, when the entity was required to have documented its review and approval of the BCS identification and classification and ended on January 31, 2018, when the entity completed its documented review and approval.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. First, the entity identified this noncompliance through an independent review of its compliance program, which is conduct that demonstrates a commitment to continuous improvement. Second, despite not having its CIP Senior Manager approve the list, the entity timely reviewed its BCS list to determine if it needed to be updated, which reduces the likelihood that the list was incorrect. ReliabilityFirst also notes that no changes occurred to the list from the previous year. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) documented CIP Sr. Manager review and approval of the entity's BES Cyber Systems Identification and Classification; 2) established a recurring annual meeting for every third Friday of January with all [REDACTED] group personnel and entity site personnel to review and certify compliance with CIP-002; 3) established a recurring annual follow-up meeting for every fourth Friday of January for the CIP Senior Manager to confirm that all required actions relating to CIP-002 and its documents have been reviewed, executed and archived appropriately; 4) revised procedure document to point to annual recurring meetings with subject matter experts and Stakeholders to ensure on-going compliance with required review and approval of BES Cyber Systems Identification and Classification; and 5) sent notification to Stakeholders that the CIP002-BES Cyber Systems Identification and Classification procedure has been revised to include reference to the standing review and approval meetings scheduled for every third and fourth Friday in January to ensure on going compliance with Requirement 2 of CIP-002-5.1a. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019262	CIP-004-6	R4	[REDACTED]	[REDACTED]	12/4/2017	12/23/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 20, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4. (The entity initially submitted the Self-Report under CIP-007-6 R5. ReliabilityFirst determined that the instance of noncompliance was not a violation of CIP-007-6 R5 but, rather, was a violation of CIP-004-6 R4.)</p> <p>On December 4, 2017, an entity subject matter expert shared passwords for NERC assets with a vendor's [REDACTED] subject matter experts prior to verifying approval of the individuals' requested access. The entity was in the process of deploying [REDACTED] software to monitor baselines for NERC assets, and the software needed to be configured with the credentials of the assets being monitored. The vendor's employees obtained read-only permissions, which they used to connect to assets to gather information for baseline purposes. The entity identified the noncompliance on December 15, 2017, during a project planning session.</p> <p>The root cause of the noncompliance was a failure to follow a process for authorizing and provisioning electronic access. This noncompliance implicates the management practice of workforce management, which includes effective training to ensure that employees understand and follow documented processes and procedures regarding confidentiality and access.</p> <p>This noncompliance started on December 4, 2017, when an entity subject matter expert shared passwords with a vendor's subject matter experts, and ended on December 23, 2017, when the entity changed the passwords for all NERC assets.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The noncompliance has the potential to affect the reliable operation of the BPS by providing an opportunity for unauthorized persons to access Bulk Electric System Cyber Systems and/or associated systems, potentially causing harm as a result of misuse or compromise. Notwithstanding, the risk was mitigated because the entity had previously performed a background check on the vendor's employees, and said employees had previously completed CIP training. Additionally, the accounts accessed by the vendor's subject matter experts were limited to read-only permissions, thus further reducing the potential risk to the BPS. Lastly, the entity promptly discovered and corrected the noncompliance. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance are distinguishable and the entity quickly identified and corrected the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) changed the passwords for the accounts that were shared with the vendor's subject matter experts; 2) updated the [REDACTED] to include use of [REDACTED] and sent updates to all subject matter experts using [REDACTED], which is a learning tool; and 3) created a standard work instruction on how to use [REDACTED] to manage shared accounts. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018710	CIP-011-2	R1	[REDACTED]	[REDACTED]	7/1/2016	9/26/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On November 17, 2017, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-011-2 R1. On September 18, 2017, during an internal review of the [REDACTED] [REDACTED]. The entity discovered 45 electronic copies of CIP protected drawings of schematics for medium impact BES Cyber Systems that were labeled as CIP Protected Information, but located outside of a CIP Information Repository (CIP Repository). Seventeen of these files were manually copied from the CIP Repository and 28 of them were PDF files that were generated for batch printing. The entity removed all of these files from the non-CIP folders by September 26, 2017.</p> <p>The root cause of this noncompliance were the responsible personnel's mistaken belief that the mapping drive was an appropriate storage location for these files and the fact that the entity's relevant procedure did not provide adequate direction to personnel. These major contributing factors involve the management practices of workforce management, which includes providing training, education, and awareness to employees, and information management, which includes ensuring the confidentiality and integrity of information.</p> <p>This noncompliance started on July 1, 2016, when the entity was required have placed these files in the CIP Repository and ended on September 26, 2017, when the entity removed all of these files from the non-CIP.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to properly protect BCSI is that the information could more easily be obtained by a malicious actor. This risk was mitigated in this case by the following factors. First, none of the assets associated with these files have external routable connectivity. Therefore, even if a malicious actor obtained the information, that person would not be able to remotely access these assets. Instead, potential malicious use of this information would require physical access to the assets. Second, these assets are physically protected as medium impact BES Cyber Systems according to the entity's Physical Security Plan, which reduces the likelihood that someone could actually gain physical access to these assets. Third, although these files were not contained in a CIP Repository, they were still located in a location that is generally secured, meaning that access is restricted to entity personnel with a current account. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance were the result of different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) moved CIP protected documents discovered during the review from non-CIP location to a designated CIP Repository; 2) conducted a stand-down with [REDACTED] to reinforce its CIP Information Protection Program; 3) conducted a stand-down with entity [REDACTED] contractors to reinforce its CIP Information Protection Program; 4) sent awareness email to all users who have access to entity [REDACTED] CIP Protected Drawings CIP Repository to reinforce its CIP Information Protection Program; 5) updated entity [REDACTED] to incorporate requirements from its CIP Information Protection Program; and 6) communicated the modification to entity [REDACTED] design related documents to entity [REDACTED]. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018770	CIP-007-6	R4	[REDACTED]	[REDACTED]	9/23/2017	9/24/2017	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On December 1, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R4. On September 23, 2017, the entity's Energy Management System (EMS) suffered a hardware failure of the primary [REDACTED]. Notification of the failure was received the next business day. At the time of the failure, all devices with agents installed automatically failed over to the secondary [REDACTED] and continued to function as usual. Devices that support more than one logging destination also automatically failed over to the secondary [REDACTED] (Thus, there was no violation for these devices.) However, the [REDACTED] servers and [REDACTED] devices had to have their logging destination manually switched over to the secondary [REDACTED] once the failure was discovered. The entity recovered logs for the [REDACTED] servers, but the [REDACTED] devices did not have logs locally stored. Furthermore, there were 20 agentless devices that lost logs from September 23, 2017, through September 25, 2017.</p> <p>The root cause of this noncompliance was the technical failure of [REDACTED]. Other contributing factors included: (a) the fact that some devices have a limited capability to store or buffer logs due to local storage capacity, which caused the inability to recover logs; and, (b) the recoveries were delayed due to a lack of pre-approved access rights, which prolonged the duration of the log loss. These contributing factors involve the management practices of asset and configuration management, which includes defining assets and their attributes, including technical limitations of the assets, risk management, in that the [REDACTED] did not have appropriate processes in place to ensure that logging would continue on all devices if the [REDACTED] failed.</p> <p>This noncompliance started on September 23, 2017, when the entity first lost logs, and ended on September 24, 2017, when logging was restored.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk of losing logging capability is that an unauthorized person could gain access to the system or insert malicious code into the system undetected. This risk was minimized in this instance because the [REDACTED] protect access to the devices at issue by [REDACTED] and [REDACTED]. Moreover, during the entire period in question, [REDACTED] This defense-in-depth strategy reduces the likelihood that any unauthorized access to the Electronic Security Perimeter (ESP) would have occurred despite the failure of logging. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance either arose from a different cause or involve conduct that ReliabilityFirst determined constitutes high frequency conduct that does not warrant an alternative disposition method.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) redirected all single-destination, agentless devices to secondary log host. The entity recovered all logs possible from agentless devices that do not send logs to multiple [REDACTED]; and 2) shared awareness of the overall system issue, summary and lessons learned with the [REDACTED] and encouraged a review of their systems to identify any similar design flaws within other systems. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018772	CIP-007-6	R4	[REDACTED]	[REDACTED]	8/23/2107	10/5/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 1, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R4. On August 23, 2017, [REDACTED] lost communications with [REDACTED] a logging aggregator, and the [REDACTED] at a remote [REDACTED]. Upon inspection, the entity discovered that the disk partition for the appliance had become corrupt and it was unable to boot. IT support staff was able to correct the issue, and when the [REDACTED] came back online, all logging was restored. However, the entity determined that the agentless devices at the site were missing logs for the period of time the [REDACTED] was offline. In total, 39 devices lost logs for the time period of August 23, 2017, through October 5, 2017. [REDACTED]</p> <p>The root cause of this noncompliance was the technical failure of [REDACTED]. Other contributing factors included: (a) the fact that some devices have a limited capability to store or buffer logs due to local storage capacity, which caused the inability to recover logs; (b) there was no secondary [REDACTED] device available to receive logs when the [REDACTED] failure occurred; and, (c) the recoveries were delayed due to a lack of pre-approved access rights, which prolonged the duration of the log loss. These contributing factors involve the management practices of asset and configuration management, which includes defining assets and their attributes, including technical limitations of the assets, risk management, in that the [REDACTED] did not have appropriate processes in place to ensure that logging would continue on all devices if the [REDACTED] failed, and workforce management, in that the duration of the issue was increased because responsible personnel did not have pre-approved access rights.</p> <p>This noncompliance started on August 23, 2017, when the entity first lost logs, and ended on October 5, 2017, when the issue was corrected and logging as restored.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk of losing logging capability is that an unauthorized person could gain access to the system or insert malicious code into the system undetected. This risk was minimized in this instance because the [REDACTED] protect access to the devices at issue by [REDACTED] and [REDACTED]. [REDACTED] This defense-in-depth strategy reduces the likelihood that any unauthorized access to the [REDACTED] would have occurred despite the failure of logging. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance either arose from a different cause or involve conduct that ReliabilityFirst determined constitutes high frequency conduct that does not warrant an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) brought the failed [REDACTED] back to operational status; 2) obtained physical access for [REDACTED] role members necessary for maintenance of equipment; 3) created an on-boarding checklist for [REDACTED] team to ensure that employees have appropriate physical access for their roles; 4) shared awareness of the overall system issue, summary and lessons learned with the [REDACTED] and encouraged a review of their systems to identify any similar design flaws within other systems; and 5) installed additional [REDACTED] device at impacted location to add addition redundancy. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019117	CIP-010-2	R2			9/17/2017	10/9/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 30, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-010-2 R2. The entity failed to monitor for changes to the baseline configuration at least once every 35 calendar days as required by CIP-010-2 R2 for two vulnerability scanner servers, which are Protected Cyber Assets (PCAs). They were not monitored because they were offline and thus the monitoring tool could not read the devices. The first asset's baseline was not monitored from August 12, 2017 through October 9, 2017 (58 calendar days) and the second asset's baseline was not monitored from August 29, 2017 through October 9, 2017 (41 calendar days).</p> <p>On October 6, 2017, the entity discovered both issues during a daily baseline monitoring reconciliation, and then resolved the issues on October 9, 2017.</p> <p>As additional background, for the first server, on August 13, 2017, during daily baseline monitoring, the entity identified a "modified" baseline for the server. "Modified" as it relates to the reporting status for the entity's monitoring tool means the configuration baseline scan shows a variance between current and last baseline (due to configuration baseline change or scanning error; or, as in this case, the reported "modification" was because the server was off-line). The entity failed to document the modification, which led to a delay in identifying the issue. Regarding the second server, on August 30, 2017, during daily baseline monitoring, the entity identified a modified baseline (again, due to the server being offline). The entity could not reconcile the change because there was not an associated change ticket. An analyst observed that the current baseline from that day matched a prior current baseline (actually the August 30, 2017 modification) and promoted the modification in [REDACTED] in error. This resulted in the entity incorrectly identifying the change as an approved change (and thus not investigating the change).</p> <p>The Self-Report notes a third instance where, in investigating the above issues on November 1, 2017, the entity noted that a change ticket opened for both assets on August 21, 2017 for re-imaging did not sufficiently identify, verify, and document cyber security controls that could be impacted by the change, nor did the entity sufficiently perform test procedures as required. ReliabilityFirst is processing this instance under a separate Violation ID as it violates a separate Requirement.</p> <p>Regarding the first instance, the root cause was inadequate communication between the manager and the owner of the baseline monitoring process to escalate the change. Regarding the second instance, the entity's process was ineffective in that it did not include a quality control check during or after completion of the work. These issues involve the management practice of verification as the entity lacked sufficient verification controls to ensure that deviations were properly and timely investigated.</p> <p>The noncompliance started on September 17, 2017, when, in the first instance, the entity should have monitored the device, through October 9, 2017, when the entity monitored both devices.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The potential risk of not monitoring baselines or documenting and investigating baseline deviations is lack of awareness of deviations that indicate a potential compromise of the asset. This risk is reduced here by the following factors. The two vulnerability scanner servers at issue here were in Electronic Security Perimeters and had other security protections in place (i.e., patching, monitoring, logging, change control, etc.) even though the baseline changes were not documented and investigated within 35 days. Additionally, the servers have a limited use and do not control Bulk Electric System Cyber Assets, which reduces the risk of compromise to the BPS. Also, the servers were not being used for vulnerability scans at the time of the issues because they were about to be upgraded. Lastly, the entity quickly self-identified and corrected the issues (within 22 days in the first instance and 5 days in the second instance). No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) documented and investigated the deviations for the affected assets as required by the entity's configuration management and baseline monitoring process; 2) conducted a meeting to identify the root causes; 3) configured [REDACTED] to automatically monitor configuration baselines for the affected assets; 4) trained teams on the method of communication between teams and escalation of un-reconcilable baseline modifications to the owner of the baseline monitoring process; 5) counseled responsible entity analysts on the requirements of the documented configuration management and baseline monitoring process, test procedures process, and change management process including the importance of following procedures; and 6) added a new procedural control requiring a peer review prior to manually promoting baselines within [REDACTED] and defining escalation path and timelines, and trained staff on the above. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019463	CIP-010-2	R1	[REDACTED]	[REDACTED]	12/1/2017	12/20/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On March 23, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-010-2 R1. On December 1, 2017, a baseline change inadvertently occurred on a Physical Access Control System (PACS) client workstation without an associated change ticket, which would have alerted entity staff to perform pre-change test procedures on the asset. The baseline changes were ultimately detected by a routine [REDACTED] scan on December 5, 2017. The entity thereafter tested the security controls and confirmed that they were not adversely affected by the change.</p> <p>The inadvertent software installation occurred because an entity analyst updated the entity's Electronic Security Perimeter [REDACTED] infrastructure to a new version. [REDACTED]</p> <p>The root cause of this noncompliance was that the [REDACTED] was not disabled on CIP-scoped PACS client workstations. Another contributing factor was that the entity analyst did not consider the PACS workstations as impacted systems when considering the downstream effects of the [REDACTED] infrastructure update. This noncompliance involves the management practice of verification, which includes ensuring changes to assets are completed as intended according to the relevant process. This noncompliance also involves the management practice of asset and configuration management, which includes defining attributes of assets and relationships between assets. Here, this would include identifying the workstations as impacted systems of the [REDACTED] infrastructure update.</p> <p>This noncompliance started on December 1, 2017, when the entity made a change without completing its required change management activities, and ended on December 20, 2017, when the entity completed the required change management activities.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. Executing changes on CIP assets without properly executing test procedures could potentially introduce vulnerabilities or system instability. However, these risks were mitigated because the entity quickly detected the noncompliance (within five days of occurrence) and thereafter quickly mitigated the noncompliance. Additionally, this noncompliance was limited to only a single PACS workstation. Thus, the noncompliance posed only minimal risk of the reliability of the BPS. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, although the current noncompliance involves conduct that is arguably similar to the previous noncompliance, the current noncompliance continues to qualify for compliance exception treatment as it involves high-frequency conduct for which the entity has demonstrated an ability to promptly identify and correct noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reviewed test procedures, verifying that security had not been compromised by the change; 2) disabled the [REDACTED] locally on all PACS workstations; 3) added a step to the procedure to specifically include PACS workstations as an impacted system for analysis; and 4) updated the installation procedure to specifically note changing the [REDACTED] to "disabled." <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020407	CIP-006-6	R1; P1.3	[REDACTED]	[REDACTED]	3/11/2018	3/11/2018	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 1, 2018, the entity submitted a self-log stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-006-6 R1.3. The entity has implemented two different physical access controls to restrict unescorted access to Physical Security Perimeters (PSPs) containing [REDACTED] (BES) Cyber Systems to only authorized personnel. The entity [REDACTED] Office is a leased high rise building that requires fire protection systems that conform to municipal ordinances and the [REDACTED] Administrative Code. In accordance with the National Fire Protection Association Life Safety Code (NFPA 101), entry points to the Physical Security Perimeter have been equipped with locking devices that upon activation of the building automatic sprinkler or fire detection system, the locking devices automatically electrically unlock door leaves in the direction of egress and remain electrically unlocked until the fire-protective system has been manually reset. Power supplies for locking devices associated with the Physical Access Control System (PACS) and the entity [REDACTED] Office are tied into electrical relays that interrupt power to these locking devices causing them to fail safe upon activation of the building's automatic sprinkler system or fire protection system.</p> <p>On the evening of Sunday, March 11, 2018, engineers who contracted with the building owner were conducting routine testing of the [REDACTED] system [REDACTED] when an alarm was generated at 7:36 p.m. in the [REDACTED] system, which in turn released the locking devices (ingress and egress) for a PSP containing High Impact BES Cyber Systems. The entity [REDACTED] received an alarm in the PACS and initiated an investigation of the cause of the alarm and response actions. Due to the investigation of the alarm and the limited availability of building security personnel, the [REDACTED] began actively monitoring access points to the impacted PSP using closed circuit television cameras. After the building owner's engineers determined the cause of the alarm, attempts were made to manually reset the [REDACTED], but the system remained in alarm state causing the doors to the PSP to remain unlocked. When it was determined that the alarm would not clear, the [REDACTED] made a request for security personnel to perform observation and access control in accordance with the entity's recovery procedures for the PACS. At 8:34 p.m., security personnel were posted to conduct monitoring and control. At 10:13 p.m. three of the four entry points were manually secured using dead bolts affixed to the doors, restricting access to a single entry point, where a security officer could monitor, control and log access using an access control list that was exported from the PACS.</p> <p>The recovery plan remained active until Tuesday, March 13, 2018 at 12:18 PM, when the alarm condition was cleared and the [REDACTED] was reset. Analysis of the issue by the building owner's [REDACTED] vendor determined that errors were made in programming the [REDACTED], which caused the persistent alarm state.</p> <p>Recovery plans for a partial loss of the PACS, developed to comply with CIP-009, were activated to limit the risk of unauthorized access to High Impact BES Cyber Systems. A review of closed circuit tv (CCTV) recording was conducted to determine if anyone gained unauthorized access to the PSP in the period beginning with the alarm activation and ending with the posting of security personnel to perform physical observation. It was determined that no unauthorized personnel gained access to the PSP.</p> <p>This noncompliance involves the management practices of reliability quality management and verification as entity staff did not have an effective process and procedure in place to ensure reporting of fire system activations to the entity [REDACTED] and to ensure coordination of system maintenance. The entity also did not verify that there were no errors in programming the [REDACTED]. Those underlying errors in programming the [REDACTED] are a root cause of this noncompliance.</p> <p>This noncompliance started on March 11, 2018, when the locking devices at the PACS were first disabled, and ended on March 11, 2018, when the entity instituted its access recovery plan to have security personnel manually check individual's access.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk posed by this noncompliance is allowing unauthorized and unescorted access into a PSP which could lead to the compromise of BES equipment. The risk is minimized because the impacted PSP is located within the entity [REDACTED] Office, where multiple layers of security exist to prevent unauthorized access to the entity's company private areas. Additionally, the PSP containing the assets is staffed 24 x 7, if an unauthorized person entered the area, the person likely would have been challenged and reported to security.</p> <p>No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) initiated the recovery plan for the impacted Physical Security Perimeter, including posting a guard; and 2) restored normal function of the PACS for the impacted Physical Security Perimeter. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020408	CIP-004-6	R4; P4.2	[REDACTED]	[REDACTED]	1/1/2018	6/19/2018	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 1, 2018, the entity submitted a self-log stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-004-6 R4.2. The entity has implemented processes to verify each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records. For unescorted physical access, the review is conducted in two phases. In the first phase, reporting managers for employees and contractors are required to attest that personnel with a reporting relationship have an ongoing need for unescorted physical access. Each Physical Security Perimeter (PSP) has a designated approving manager for access. During the second phase, the approving managers are presented with lists of personnel with unescorted access privileges to PSPs for which they are responsible. The approving managers review and approve the access lists closing out the quarterly process.</p> <p>On May 30, 2018, during a routine internal review of compliance evidence, it was discovered that some evidence related to quarterly verifications of unescorted physical records completed during the fourth calendar quarter of 2017 and the first calendar quarter of 2018 were missing from the designated evidence repository. Upon conducting a detailed review, it was determined that the missing records were limited to three PSPs that are managed by the same approving manager. While the entity believes that the verification process was completed, the entity did not have the required evidence to demonstrate compliance.</p> <p>A review of compliance evidence related to physical access authorization verifications was conducted to verify the extent of missing documentation. All compliance records were reviewed and verified for all other quarters reviewed, including the quarter immediately prior to the fourth calendar quarter of 2017 and the quarter immediately following the first calendar quarter of 2018.</p> <p>Going forward, a checklist and sign-off process will be implemented to validate that the verification has been completed and all compliance evidence has been stored in the designated repository.</p> <p>This noncompliance involves the management practices of reliability quality management and validation. The entity's process for validating access records did not include an internal control to validate that the verification has been completed and that all compliance evidence has been stored in the designated repository. That process weakness and lack of a validation internal control are both root causes of this noncompliance.</p> <p>This noncompliance started on January 1, 2018, when the entity discovered that it did not have evidence related to quarterly verifications of unescorted physical records completed during the fourth calendar quarter of 2017 and the first calendar quarter of 2018 for three PSPs and ended on June 19, 2018 when the entity completed the review and verification for the second calendar quarter of 2018 for these three PSPs.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk posed by this noncompliance is allowing unauthorized and unescorted access into a PSP which could lead to the compromise of Bulk Electric System (BES) equipment. The risk is minimized because the quarterly review process is a compliance control and not performing the quarterly review process would not result in unauthorized personnel gaining unescorted physical access to BES Cyber Systems. Additionally, all compliance records were reviewed and verified for the quarter immediately prior to the fourth calendar quarter of 2017 and all compliance records were reviewed and verified for the quarter immediately following the first calendar quarter of 2018.</p> <p>No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) implemented a process which requires the [REDACTED] to complete a checklist to assure evidence of the quarterly unescorted physical access authorization reviews are uploaded to the compliance repository; and 2) implemented a process improvement to have a second person verify that records of quarterly access authorizations reviews are uploaded to the compliance repository. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020409	CIP-006-6	R1; P1.3	[REDACTED]	[REDACTED]	7/9/2018	7/11/2018	Self-Log	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On August 1, 2018, the entity submitted a self-log stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-006-6 R1.3. The entity has implemented two different physical access controls to restrict unescorted access to Physical Security Perimeters containing [REDACTED] Bulk Electric System (BES) Cyber Systems to only authorized personnel. The entity facilities are required to have fire protection systems that conform to municipal ordinances and the [REDACTED] Administrative Code. In accordance with the National Fire Protection Association Life Safety Code (NFPA) [REDACTED] entry points to the Physical Security Perimeter (PSP) have been equipped with locking devices that upon activation of the building automatic sprinkler or fire detection system automatically and electrically unlock door leaves in the direction of egress. These devices remain electrically unlocked until the fire-protective system has been manually reset. Power supplies for locking devices associated with the Physical Access Control System (PACS) and the entity buildings [REDACTED] are tied into electrical relays that interrupt power to the locking devices causing them to fail safe upon activation of the building's fire protection system.</p> <p>In the first instance, on Monday July 9, 2018 at 6:00 a.m. a fire alarm was activated at the [REDACTED], which caused electrical relays to interrupt power to locking devices at entry points to two separate Physical Security Perimeters (PSPs). The PSP doors were unlocked in both directions. The doors are equipped with magnetic locks, which require power to be applied constantly to maintain a secure state. When a fire alarm signal is activated, the tie mechanism interrupts power to the magnetic lock, causing the door to be in an unsecure state. In this state, the lever set can be operated for both egress and entry. This is required to assure personnel can safely egress the area in the event of an actual alarm. The logging functions of the PACS remain operational; the system will report alarms, as well as, log access attempts if a card is presented to the reader. First responders and entity personnel investigated the cause of the alarm and the site was given an all clear to resume normal operations at 6:35 a.m. The entity [REDACTED] was advised of the alarm condition and state of the locking devices at 06:45 a.m. and initiated recovery plans associated with the loss of access control at a PSP. The system was successfully reset and normal operation of locally mounted PACS hardware resumed at 9:48 a.m.</p> <p>In the second instance, on Wednesday July 11, 2018 the fire protection system at the [REDACTED] was being serviced by a vendor. At 1:00 p.m. it was discovered that the entry points to two separate Physical Security Perimeters were unlocked. The PSP doors were unlocked in both directions. The doors are equipped with magnetic locks, which require power to be applied constantly to maintain a secure state. When a fire alarm signal is activated, the tie mechanism interrupts power to the magnetic lock, causing the door to be in an unsecure state. In this state, the lever set can be operated for both egress and entry. This is required to assure personnel can safely egress the area in the event of an actual alarm. The logging functions of the PACS remain operational; the system will report alarms, as well as, log access attempts if a card is presented to the reader. The vendor who services the [REDACTED] system was installing additional detection devices. One of the newly installed devices was triggering the activation of the release mechanism, without putting the entire system into alarm. The entity [REDACTED] was notified and initiated recovery plans associated with the loss of access control at a PSP. As part of the response process, the [REDACTED] dispatched a technician to troubleshoot and repair the issue, and supplemental security coverage was requested to perform physical observation. The technician arrived to troubleshoot and begin repairs of the PACS at 2:00 p.m., and a security officer arrived at the facility at 3:20 p.m. to perform physical observation. It was determined that the fire safety systems relays were active and interrupted power to locking devices at entry points to the impacted Physical Security Perimeters. Repairs were executed and normal operation of locally mounted PACS hardware resumed at 5:00 p.m.</p> <p>A review of closed circuit tv (CCTV) recording was conducted to determine if anyone gained unauthorized access to the PSP during the time periods when power to locking devices was interrupted. It was determined that no unauthorized personnel gained access to the PSPs.</p> <p>This noncompliance involves the management practices of reliability quality management and work management as entity staff did not have an effective process and procedure in place to ensure reporting of fire system activations to the entity [REDACTED] and to ensure coordination of system maintenance. That lack of an effective process/procedure to coordinate fire system activations with the [REDACTED] is a root cause of this noncompliance.</p> <p>There are two separate instances in this noncompliance. The first instance started on July 9, 2018, when the locking devices at the PACS were first disabled because of the fire alarm and ended on July 9, 2018, when the entity re-enabled the locking devices at the PACS and normal operation of the PACS resumed. The second instance started on July 11, 2018 when the locking devices at the PACS were disabled because of the fire alarm and ended on July 11, 2018, when the entity re-enabled the locking devices at the PACS and normal operation of the PACS resumed.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk posed by this noncompliance is allowing unauthorized and unescorted access into a PSP which could lead to the compromise of BES equipment. The risk is minimized because the impacted PSPs are located within an entity facility where multiple layers of security exist to prevent unauthorized access to company private areas. [REDACTED]</p> <p>[REDACTED] Additionally, CCTV cameras are used as a management and investigative tool and afford [REDACTED] personnel with monitoring capabilities. Additionally, based on CCTV review of the PSPs, there was no unauthorized physical access to the PSPs.</p> <p>No harm is known to have occurred.</p>					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020409	CIP-006-6	R1; P1.3	[REDACTED]	[REDACTED]	7/9/2018	7/11/2018	Self-Log	Completed
Mitigation			To mitigate this noncompliance, the entity: <ol style="list-style-type: none"> 1) initiated the recovery plan for the impacted Physical Security Perimeters; 2) restored normal function of the PACS for the impacted Physical Security Perimeters; 3) initiated the recovery plan for the impacted Physical Security Perimeters; 4) restored normal function of the PACS for the impacted Physical Security Perimeters; 5) discussed measures with [REDACTED] staff to enhance reporting of fire system activations to the entity [REDACTED] and coordination of system maintenance; and 6) implemented measures to enhance reporting of fire system activations to the entity [REDACTED] and coordination of system maintenance. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020410	CIP-007-6	R5 P5.4	[REDACTED]	[REDACTED]	7/23/2018	7/26/2018	Self-Log	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 1, 2018, the entity submitted a self-log stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-007-6 R5.4. On July 23, 2018, during the cyber vulnerability assessment (CVA) of the [REDACTED] control house, it was identified that one (1) microprocessor relay level one password was unchanged from the default password. The correct level one password was applied to the relay on July 26, 2018 once the proper clearances were obtained to safely perform the work. This type of relay has a level one and a level two password. Level one access only allows for viewing of settings, power quality, and status. The level two access permits change and control functions for this relay. The level two password was found to be the appropriate non-default password for this relay.</p> <p>New stations are baselined prior to commissioning, and then added to the CVA schedule for the following year. The [REDACTED] is a newly constructed facility which was commissioned in [REDACTED] and contains a total of 94 microprocessor relays. The baseline review, which includes documenting the baseline and performing password changes for this relay was performed on [REDACTED]. As a result of this default password finding during the CVA, an investigation was conducted by the entity's [REDACTED] that concluded that the Relay Technician performing the work on the relay neglected to confirm the non-default password was saved by the relay. The responsible Relay Technician was counseled on the importance of password change verification.</p> <p>Due to a similar, previous self-log (see [REDACTED]), the entity completed a procedure revision to ensure password changes are appropriately applied. The procedure revision was completed on [REDACTED] two weeks after the baseline of this relay was performed. This procedure revision incorporates a step to perform a second login into the relay after the passwords are changed in order to verify that all changes were accepted and saved by the relay.</p> <p>[REDACTED] has 94 Bulk Electric System relays installed and this relay was the only issue found during the CVA. In addition to [REDACTED] the entity has a total of 29 medium impact stations containing a total of 1,258 active relays. There are 2 medium impact stations left in the original CVA schedule for 2018 to have a CVA completed. Due to this issue, the entity has added any new stations initially baselined to date in 2018 that would normally be a part of the 2019 CVA schedule to the CVA schedule for this year. This change brought one additional station into the CVA schedule for 2018. Additionally, the entity has changed the CVA schedule due date from end of September to a more aggressive completion date of August 24, 2018 for these remaining 3 stations in the revised schedule.</p> <p>This noncompliance involves the management practices of reliability quality management and workforce management. The procedure used to determine when password changes were necessary left room for improvement and the entity completed a procedure revision to ensure all password changes are appropriately applied. The Relay Technician performing the work on the relay at issue neglected to confirm the non-default password was saved by the relay because he was ineffectively trained on the importance of password change verification. A root cause of this noncompliance was the ineffective procedure.</p> <p>This noncompliance started on July 23, 2018, when the entity discovered that the default password was still in place on this relay while conducting its annual CVA and ended on July 26, 2018, when the entity changed the default password on the relay.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed by leaving a default password in place is a reduced level of protection, making it easier for a bad actor to access and compromise the relay that the password is designed to protect. This noncompliance posed a minimal risk to the BPS because the level one password access only allows for viewing of settings, power quality, and status. The level two password had already been changed to the appropriate CIP non-default password. Level two access permits change and control functions for this relay. Additionally these relays do not have external routable connectivity and are maintained within a PSP.</p> <p>No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) corrected the level 1 password on the relay; 2) held a counselling session with the responsible Relay Technician to stress the importance of password change verification; and 3) completed the CVAs of all medium impact substations, including new stations, to insure no other default password issues exist in the entity's medium impact substations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019275	CIP-004-6	R4	[REDACTED]	[REDACTED]	12/12/2017	1/12/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 23, 2018, [REDACTED] and [REDACTED] through [REDACTED] submitted a Self-Report stating that, as a [REDACTED] [REDACTED] [REDACTED] and [REDACTED] they were in noncompliance with CIP-004-6 R4. [REDACTED] [REDACTED] [REDACTED].</p> <p>On December 12, 2017, an IT Security contractor for the entity erroneously granted an engineer access rights to Bulk Electric System (BES) Cyber Security Information (BCSI). (Though the engineer had previously been granted access (on 08/01/2016) to some CIP-protected information, that access was removed on 08/25/2016. As such, his personnel risk assessment was current and information protection training was taken at the time.) On January 12, 2018, the entity discovered the error while preparing enrollment lists for annual cybersecurity training and immediately revoked the unintended access rights. (After locating no request for access and no record of the necessary authorization, the unintended access rights were immediately revoked at 2:32pm.) An after-the-fact review yielded no evidence that the engineer accessed or attempted to access CIP-protected information. The engineer did not know that the unintended access rights had been granted, and access to the most sensitive information was read-only, so there was no ability to delete or edit records.</p> <p>This noncompliance involves the management practice of workforce management, which includes effective training to ensure employees understand and follow documented procedures. The root cause of the noncompliance was failing to follow approved processes and procedures. The IT Security contractor did not follow the correct process when he erroneously granted an engineer access rights to BCSI.</p> <p>This noncompliance started on December 12, 2017, when the access was granted without proper authorization, and ended on January 12, 2018, when the entity revoked the unintended access rights.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The noncompliance has the potential to affect the reliable operation of the BPS by providing an opportunity for unauthorized personnel to access BES Cyber Systems and associated systems. Notwithstanding, the risk was minimized because the engineer who was granted unauthorized access had previously been granted access to CIP-protected information. Therefore, the engineer had completed CIP training and had a valid Personnel Risk Assessment, thus reducing the risk of compromise to the BPS.</p> <p>No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance are distinguishable from the instant noncompliance and the entity promptly self-identified and mitigated the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) counseled the IT Security contractor on the need to follow the documented process for granting access to BCSI; 2) implemented a technical control to restrict the ability to change membership of [REDACTED] groups used to control access to BCSI and allow only core IT Security employees to make such membership changes; 3) counseled the CIP Compliance Team employee on the appropriate process to follow when receiving an alert in the CIP Compliance team group mailbox; and 4) enhanced the process, which detects changes to these [REDACTED] groups to automatically generate a trouble ticket rather than email when changes are detected. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019277	CIP-006-6	R1	[REDACTED]	[REDACTED]	1/10/2018	1/11/2018	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On February 23, 2018, [REDACTED] and [REDACTED] through [REDACTED] submitted a Self-Report stating that, as a [REDACTED] [REDACTED] [REDACTED] and [REDACTED] they were in noncompliance with CIP-006-6 R1. [REDACTED]</p> <p>On January 10, 2018, an entity senior IT infrastructure consultant (Infrastructure Consultant) on the [REDACTED] [REDACTED] [REDACTED] Team opened a secure Physical Security Perimeter (PSP) cabinet, and subsequently left the area without re-securing the cabinet. The cabinet is located inside a card-reader-protected server room inside a building that requires company identification to enter. Video records reveal that the PSP cabinet was left unattended for 16 minutes.</p> <p>Similarly, on January 11, 2018, the Infrastructure Consultant again accessed and then left the same PSP cabinet without re-securing it. This time, a central alarm station security officer (Security Officer) observed the Infrastructure Consultant leave the PSP cabinet without re-securing it via video monitors. After observing this, the Security Officer notified a Principal Security Consultant, who then went to the server room, secured the PSP cabinet door, and waited for the Infrastructure Consultant to return. The Infrastructure Consultant returned a few minutes later. Video records confirm the PSP cabinet was left unattended on January 11, 2018 for 22 minutes (from the time the Infrastructure Consultant left until the time the Principal Security Consultant entered the server room and secured the PSP cabinet door).</p> <p>On January 12, 2018, the Principal Security Consultant reported this incident to the CIP Compliance Team. The CIP Compliance Team performed an extensive investigation by analyzing relevant card-reader logs, door-held-open alarms, central alarm station incident reports, and video records. The video records indicate that no one else entered the area while the cabinet was open and unattended. (The Manager [REDACTED] visited the area and verified that all appropriate NERC CIP Physical Security Perimeter signage was in place.)</p> <p>This noncompliance involves the management practice of workforce management through ineffective training. The Infrastructure Consultant did not realize that the server cabinet doors could not be left open and unattended. That ineffective training is a root cause of this noncompliance.</p> <p>This noncompliance started on January 10, 2018, when the Infrastructure Consultant first left the PSP cabinet unattended without re-securing it and ended on January 11, 2018, when the Principal Security Consultant secured the PSP cabinet door.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is allowing an unauthorized individual the ability to access the PSP cabinet. The risk is minimized because the cabinet is located inside a card-reader protected server room that few individuals can access. The cabinet was also left unsecured and unattended for short amounts of time: 16 minutes in the first instance and 22 minutes in the second instance. Lastly, ReliabilityFirst notes that the entity reviewed video records and confirmed that no other personnel (except the Principal Security Consultant who re-secured the cabinet) were in the area during the times the cabinet was left unattended.</p> <p>No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance are distinguishable from the instant noncompliance and the entity promptly self-identified and mitigated the instant noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) counseled the Infrastructure Consultant on the proper procedures for maintaining security of equipment cabinets identified as PSPs; and 2) distributed a targeted security awareness bulletin to all personnel who have access to a PSP explaining the requirements for working in the cabinets as well as the risks of unmet expectations. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019276	CIP-010-2	R1	[REDACTED]	[REDACTED]	1/12/2018	1/16/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 23, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] [REDACTED] [REDACTED] and [REDACTED] it was in noncompliance with CIP-010-2 R1. On January 16, 2018, the entity's CIP Compliance team discovered that the baseline configurations of 14 workstations had not been updated within the 30-day period required by CIP-010-2 after certain security patches were installed on December 13, 2017. Upon discovery, four days after the deadline had passed, the entity immediately updated the configurations.</p> <p>The initial delay in updating the entity's baselines configurations stems from a problematic installation of certain [REDACTED] security patches on December 13, 2017 and the subsequent investigation of that issue. Specifically, the entity failed to install the patches correctly on three workstations and that prevented the entity's configuration monitoring tool ([REDACTED] [REDACTED]) from detecting the related configuration baseline exceptions the morning after they were installed.</p> <p>This triggered an internal investigation into what prevented [REDACTED] [REDACTED] recognition of the exceptions on the affected workstations. The entity completed the investigation on December 26, 2017, but due to the limited availability of key personnel between Christmas and the new year, the entity did not take the final corrective actions until the first week of January. By focusing too much on addressing the issues caused by the December 13 installation of the aforementioned security patches, the CIP Compliance team lost track of the need to update the configuration baselines for the remaining 14 workstations within 30 days.</p> <p>Operator error in updating a spreadsheet that the entity uses to track the status of all baseline configuration exceptions each week also contributed to the delay. The spreadsheet will issue a warning whenever the baseline configuration is not updated within 22 days of installation. This is designed to provide the CIP Compliance team with eight days to complete the configuration update before the 30-day requirement is exceeded. However, in this case, a new member of the CIP Compliance team was tasked with entering the necessary data into the spreadsheet, but did so incorrectly, which prevented the spreadsheet from alerting the CIP Compliance team that the 30-day deadline was approaching.</p> <p>This noncompliance involves the management practices of workforce management and work management. Workforce management through ineffective training is involved because the individual responsible for updating the spreadsheet that the entity uses to track the status of all baseline configurations exceptions each week entered the necessary data into the spreadsheet incorrectly, which prevented the Spreadsheet from alerting the CIP Compliance team that the 30-day deadline was approaching. That ineffective training is a root cause of this noncompliance. Work management is involved because the CIP Compliance Team got preoccupied with resolving the issues caused by the December 13, 2017 patch installation and that allowed them to lose track of the need to update the configuration baselines within 30 days. That preoccupation and the lack of an effective control to remind the CIP Compliance team of the need to update the configuration baselines is a contributing cause of this noncompliance.</p> <p>This noncompliance started on January 12, 2018, when the entity failed to update the baseline configurations of 14 workstations within the 30-day period required by CIP-010-2 after certain security patches were installed on December 13, 2017 and ended on January 16, 2018, when the entity updated the overdue baseline configurations.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is permitting a change to be implemented without updating the corresponding baseline configurations and that could adversely affect system security. The risk is minimized because the configuration baseline updates were applied only four days late. The entity quickly identified, assessed, and corrected this issue, which evidences strong detective and corrective controls. Additionally, all of the configuration baseline changes were properly authorized.</p> <p>No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance are distinguishable from the instant noncompliance and the entity promptly self-identified and mitigated the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) counseled the employees involved on the importance of accuracy and attention to detail; 2) updated the procedure used to generate the report to specify how data is to be entered into the entity's internal monitoring tool; 3) enhanced the monitoring tool and report template to look for corrupted data and to issue warnings if data corruption is found; and 4) enhanced the report template by updating the header area of the template to include an area to document the name of the person who generated the report and the oldest date observed in the report. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019506	CIP-010-2	R1	[REDACTED]	[REDACTED]	1/5/2018	2/12/2018	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On March 28, 2018, [REDACTED] and [REDACTED] through [REDACTED] submitted a Self-Report stating that, as a [REDACTED] [REDACTED] [REDACTED] and [REDACTED] they were in noncompliance with CIP-010-2 R1. [REDACTED]</p> <p>On January 5, 2018, the entity unintentionally installed [REDACTED] software upgrades on two Physical Access Control Systems (PACS) before completing the requisite assessment, verification, and documentation of the potential impact to CIP-005 and CIP-007 security controls. Additionally, the entity did not timely update baseline configurations to reflect the installation of these upgrades. These issues affected two of the entity's 50 CIP servers that had the [REDACTED] software updates installed.</p> <p>The individual responsible for installing the [REDACTED] updates (an IT SME) recognized that the affected servers required manual deployment. The IT SME, however, mistakenly included the two PACS servers with a large group of corporate servers that already had the [REDACTED] upgrade automatically installed. That resulted in the upgrades being prematurely installed on these two PACS servers.</p> <p>The entity discovered this issue on January 24, 2018 while processing baseline updates for unrelated security patches that were accepted into the baseline configuration that day.</p> <p>Additionally, the entity did not update the baseline configuration to reflect installation of the [REDACTED] software updates within 30 days as required by CIP-010-2 R1. The baseline configurations were not updated because the individual responsible for applying the updates failed to create an incident record to investigate the updates as required by the entity's documented procedures. Without an incident record to drive timely resolution, the investigation of the [REDACTED] software exceptions lasted 38 days. By accepting the baseline configuration for the unrelated security patch exemptions, the [REDACTED] for the [REDACTED] software update reported in [REDACTED] [REDACTED] incorrectly changed from 1/05/2018 to 1/24/2018 due to a software flaw. This field is used to trigger a warning in a weekly report run by the entity to determine when the baseline configuration is not updated within 22 days of installation. The incorrect date change rendered this control ineffective and the entity did not meet the 30-day requirement.</p> <p>On February 12, 2018, the entity completed the investigation into the [REDACTED] software baseline exceptions and the entity updated the related baseline configurations. The configurations were updated eight days late.</p> <p>This noncompliance involves the management practices of workforce management and verification. Workforce management through ineffective training is involved because the IT SME incorrectly placed the two PACS servers in the wrong deployment group for the [REDACTED] update. Also, the CIP individual failed to create an incident report, which hampered the entity's subsequent investigation of the [REDACTED] exceptions. Ineffective training of both individuals is a root cause of this noncompliance. Verification is involved because the entity did not verify that the correct installation date for the software was being used in [REDACTED] [REDACTED] to track the 30-day baseline update requirement. That failure to verify is a contributing cause of this noncompliance.</p> <p>This noncompliance started on January 5, 2018, when the entity unintentionally installed [REDACTED] software upgrades on two PACS before completing the requisite assessment, verification, and documentation of the upgrades potential impact to CIP-005 and CIP-007 security controls and ended on February 12, 2018, when the entity updated the related baseline configurations eight days late.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is twofold. First, executing changes on CIP assets without properly executing test procedures could potentially introduce vulnerabilities or system instability. Second, not maintaining accurate baselines has the potential to affect the reliability of the bulk electric system by reducing the entity's ability to identify unauthorized activity, changes, or vulnerabilities and by introducing system instability when making changes to assets. The risk is minimized because the [REDACTED] software upgrades were previously approved and intended to be applied to these two PACS servers, they were just prematurely installed. The risk is further minimized because the configuration baseline changes were all authorized and the configuration baselines were only updated eight days late.</p> <p>No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance are distinguishable from the instant noncompliance and the entity promptly self-identified and mitigated the instant noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) created a new [REDACTED] server management group specific to the PACS servers in order to minimize the chance that they will be mismanaged in the future; 2) counseled the IT subject matter expert on the importance of adherence to documented procedures, the importance of communicating widespread changes to all impacted areas, and the importance of attention to detail and accuracy in work related to NERC CIP applicable systems; 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019506	CIP-010-2	R1	[REDACTED]	[REDACTED]	1/5/2018	2/12/2018	Self-Report	Completed
			<p>3) counseled the CIP Team Member on the importance of adhering to documented procedures and of using incident records to track investigation and resolution of potential issues; and</p> <p>4) updated the procedure for tracking the baseline to ensure that any configuration exceptions which are not accepted into the baseline are clearly documented in an incident record whose target completion date is less than thirty days from the original "[REDACTED]" before accepting any exceptions. The entity also reviewed a report of such incident records weekly at the same time the [REDACTED] is reviewed.</p> <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019278	CIP-004-6	R4	██████████	██████████	12/12/2017	1/12/2018	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On February 23, 2018, ██████████ submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-004-6 R4.</p> <p>On December 12, 2017, an IT Security contractor for the entity erroneously granted an engineer access rights to Bulk Electric System (BES) Cyber Security Information (BCSI). (Though the engineer had previously been granted access (on 08/01/2016) to some CIP-protected information, that access was removed on 08/25/2016. As such, his personnel risk assessment was current and information protection training was taken at the time.) On January 12, 2018, the entity discovered the error while preparing enrollment lists for annual cybersecurity training and immediately revoked the unintended access rights. (After locating no request for access and no record of the necessary authorization, the unintended access rights were immediately revoked at 2:32pm.) An after-the-fact review yielded no evidence that the engineer accessed or attempted to access CIP-protected information. The engineer did not know that the unintended access rights had been granted, and access to the most sensitive information was read-only, so there was no ability to delete or edit records.</p> <p>This noncompliance involves the management practice of workforce management, which includes effective training to ensure employees understand and follow documented procedures. The root cause of the noncompliance was failing to follow approved processes and procedures. The IT Security contractor did not follow the correct process when he erroneously granted an engineer access rights to BCSI.</p> <p>This noncompliance started on December 12, 2017, when the access was granted without proper authorization, and ended on January 12, 2018, when the entity revoked the unintended access rights.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The noncompliance has the potential to affect the reliable operation of the BPS by providing an opportunity for unauthorized personnel to access BES Cyber Systems and associated systems. Notwithstanding, the risk was minimized because the engineer who was granted unauthorized access had previously been granted access to CIP-protected information. Therefore, the engineer had completed CIP training and had a valid Personnel Risk Assessment, thus reducing the risk of compromise to the BPS.</p> <p>No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance are distinguishable from the instant noncompliance and the entity promptly self-identified and mitigated the instant noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) counseled the IT Security contractor on the need to follow the documented process for granting access to BCSI; 2) implemented a technical control to restrict the ability to change membership of ██████████ groups used to control access to BCSI and allow only core IT Security employees to make such membership changes; 3) counseled the CIP Compliance Team employee on the appropriate process to follow when receiving an alert in the CIP Compliance team group mailbox; and 4) enhanced the process, which detects changes to these ██████████ groups to automatically generate a trouble ticket rather than email when changes are detected. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019280	CIP-006-6	R1	[REDACTED]	[REDACTED]	1/10/2018	1/11/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 23, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-006-6 R1.</p> <p>On January 10, 2018, an entity senior IT infrastructure consultant (Infrastructure Consultant) on the [REDACTED] Team opened a secure Physical Security Perimeter (PSP) cabinet, and subsequently left the area without re-securing the cabinet. The cabinet is located inside a card-reader-protected server room inside a building that requires company identification to enter. Video records reveal that the PSP cabinet was left unattended for 16 minutes.</p> <p>Similarly, on January 11, 2018, the Infrastructure Consultant again accessed and then left the same PSP cabinet without re-securing it. This time, a central alarm station security officer (Security Officer) observed the Infrastructure Consultant leave the PSP cabinet without re-securing it via video monitors. After observing this, the Security Officer notified a Principal Security Consultant, who then went to the server room, secured the PSP cabinet door, and waited for the Infrastructure Consultant to return. The Infrastructure Consultant returned a few minutes later. Video records confirm the PSP cabinet was left unattended on January 11, 2018 for 22 minutes (from the time the Infrastructure Consultant left until the time the Principal Security Consultant entered the server room and secured the PSP cabinet door).</p> <p>On January 12, 2018, the Principal Security Consultant reported this incident to the CIP Compliance Team. The CIP Compliance Team performed an extensive investigation by analyzing relevant card-reader logs, door-held-open alarms, central alarm station incident reports, and video records. The video records indicate that no one else entered the area while the cabinet was open and unattended. (The Manager [REDACTED] visited the area and verified that all appropriate NERC CIP Physical Security Perimeter signage was in place.)</p> <p>This noncompliance involves the management practice of workforce management through ineffective training. The Infrastructure Consultant did not realize that the server cabinet doors could not be left open and unattended. That ineffective training is a root cause of this noncompliance.</p> <p>This noncompliance started on January 10, 2018, when the Infrastructure Consultant first left the PSP cabinet unattended without re-securing it and ended on January 11, 2018, when the Principal Security Consultant secured the PSP cabinet door.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is allowing an unauthorized individual the ability to access the PSP cabinet. The risk is minimized because the cabinet is located inside a card-reader protected server room that few individuals can access. The cabinet was also left unsecured and unattended for short amounts of time: 16 minutes in the first instance and 22 minutes in the second instance. Lastly, ReliabilityFirst notes that the entity reviewed video records and confirmed that no other personnel (except the Principal Security Consultant who re-secured the cabinet) were in the area during the times the cabinet was left unattended.</p> <p>No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance are distinguishable from the instant noncompliance and the entity promptly self-identified and mitigated the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) counseled the Infrastructure Consultant on the proper procedures for maintaining security of equipment cabinets identified as PSPs; and 2) distributed a targeted security awareness bulletin to all personnel who have access to a PSP explaining the requirements for working in the cabinets as well as the risks of unmet expectations. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019279	CIP-010-2	R1	██████████	██████████	1/12/2018	1/16/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 23, 2018, ██████████ submitted a Self-Report stating that, as a ██████████ ██████████ ██████████ and ██████████ it was in noncompliance with CIP-010-2 R1. On January 16, 2018, the entity's CIP Compliance team discovered that the baseline configurations of 14 workstations had not been updated within the 30-day period required by CIP-010-2 after certain security patches were installed on December 13, 2017. Upon discovery, four days after the deadline had passed, the entity immediately updated the configurations.</p> <p>The initial delay in updating the entity's baselines configurations stems from a problematic installation of certain ██████████ security patches on December 13, 2017 and the subsequent investigation of that issue. Specifically, the entity failed to install the patches correctly on three workstations and that prevented the entity's configuration monitoring tool ██████████ ██████████ from detecting the related configuration baseline exceptions the morning after they were installed.</p> <p>This triggered an internal investigation into what prevented ██████████ recognition of the exceptions on the affected workstations. The entity completed the investigation on December 26, 2017, but due to the limited availability of key personnel between Christmas and the new year, the entity did not take the final corrective actions until the first week of January. By focusing too much on addressing the issues caused by the December 13 installation of the aforementioned security patches, the CIP Compliance team lost track of the need to update the configuration baselines for the remaining 14 workstations within 30 days.</p> <p>Operator error in updating a spreadsheet that the entity uses to track the status of all baseline configuration exceptions each week also contributed to the delay. The spreadsheet will issue a warning whenever the baseline configuration is not updated within 22 days of installation. This is designed to provide the CIP Compliance team with eight days to complete the configuration update before the 30-day requirement is exceeded. However, in this case, a new member of the CIP Compliance team was tasked with entering the necessary data into the spreadsheet, but did so incorrectly, which prevented the spreadsheet from alerting the CIP Compliance team that the 30-day deadline was approaching.</p> <p>This noncompliance involves the management practices of workforce management and work management. Workforce management through ineffective training is involved because the individual responsible for updating the spreadsheet that the entity uses to track the status of all baseline configurations exceptions each week entered the necessary data into the spreadsheet incorrectly, which prevented the Spreadsheet from alerting the CIP Compliance team that the 30-day deadline was approaching. That ineffective training is a root cause of this noncompliance. Work management is involved because the CIP Compliance Team got preoccupied with resolving the issues caused by the December 13, 2017 patch installation and that allowed them to lose track of the need to update the configuration baselines within 30 days. That preoccupation and the lack of an effective control to remind the CIP Compliance team of the need to update the configuration baselines is a contributing cause of this noncompliance.</p> <p>This noncompliance started on January 12, 2018, when the entity failed to update the baseline configurations of 14 workstations within the 30-day period required by CIP-010-2 after certain security patches were installed on December 13, 2017 and ended on January 16, 2018, when the entity updated the overdue baseline configurations.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is permitting a change to be implemented without updating the corresponding baseline configurations and that could adversely affect system security. The risk is minimized because the configuration baseline updates were applied only four days late. The entity quickly identified, assessed, and corrected this issue, which evidences strong detective and corrective controls. Additionally, all of the configuration baseline changes were properly authorized.</p> <p>No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance are distinguishable from the instant noncompliance and the entity promptly self-identified and mitigated the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) counseled the employees involved on the importance of accuracy and attention to detail; 2) updated the procedure used to generate the report to specify how data is to be entered into the entity's internal monitoring tool; 3) enhanced the monitoring tool and report template to look for corrupted data and to issue warnings if data corruption is found; and 4) enhanced the report template by updating the header area of the template to include an area to document the name of the person who generated the report and the oldest date observed in the report. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019507	CIP-010-2	R1	██████████	██████████	1/5/2018	2/12/2018	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On March 28, 2018, ██████████ submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-010-2 R1.</p> <p>On January 5, 2018, the entity unintentionally installed ██████████ software upgrades on two Physical Access Control Systems (PACS) before completing the requisite assessment, verification, and documentation of the potential impact to CIP-005 and CIP-007 security controls. Additionally, the entity did not timely update baseline configurations to reflect the installation of these upgrades. These issues affected two of the entity's 50 CIP servers that had the ██████████ software updates installed.</p> <p>The individual responsible for installing the ██████████ updates (an IT SME) recognized that the affected servers required manual deployment. The IT SME, however, mistakenly included the two PACS servers with a large group of corporate servers that already had the ██████████ upgrade automatically installed. That resulted in the upgrades being prematurely installed on these two PACS servers.</p> <p>The entity discovered this issue on January 24, 2018 while processing baseline updates for unrelated security patches that were accepted into the baseline configuration that day.</p> <p>Additionally, the entity did not update the baseline configuration to reflect installation of the ██████████ software updates within 30 days as required by CIP-010-2 R1. The baseline configurations were not updated because the individual responsible for applying the updates failed to create an incident record to investigate the updates as required by the entity's documented procedures. Without an incident record to drive timely resolution, the investigation of the ██████████ software exceptions lasted 38 days. By accepting the baseline configuration for the unrelated security patch exemptions, the '██████████' for the ██████████ software update reported in ██████████ ██████████ incorrectly changed from 1/05/2018 to 1/24/2018 due to a software flaw. This field is used to trigger a warning in a weekly report run by the entity to determine when the baseline configuration is not updated within 22 days of installation. The incorrect date change rendered this control ineffective and the entity did not meet the 30-day requirement.</p> <p>On February 12, 2018, the entity completed the investigation into the ██████████ software baseline exceptions and the entity updated the related baseline configurations. The configurations were updated eight days late.</p> <p>This noncompliance involves the management practices of workforce management and verification. Workforce management through ineffective training is involved because the IT SME incorrectly placed the two PACS servers in the wrong deployment group for the ██████████ update. Also, the CIP individual failed to create an incident report, which hampered the entity's subsequent investigation of the ██████████ exceptions. Ineffective training of both individuals is a root cause of this noncompliance. Verification is involved because the entity did not verify that the correct installation date for the software was being used in ██████████ ██████████ to track the 30-day baseline update requirement. That failure to verify is a contributing cause of this noncompliance.</p> <p>This noncompliance started on January 5, 2018, when the entity unintentionally installed ██████████ software upgrades on two PACS before completing the requisite assessment, verification, and documentation of the upgrades potential impact to CIP-005 and CIP-007 security controls and ended on February 12, 2018, when the entity updated the related baseline configurations eight days late.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is twofold. First, executing changes on CIP assets without properly executing test procedures could potentially introduce vulnerabilities or system instability. Second, not maintaining accurate baselines has the potential to affect the reliability of the bulk electric system by reducing the entity's ability to identify unauthorized activity, changes, or vulnerabilities and by introducing system instability when making changes to assets. The risk is minimized because the ██████████ software upgrades were previously approved and intended to be applied to these two PACS servers, they were just prematurely installed. The risk is further minimized because the configuration baseline changes were all authorized and the configuration baselines were only updated eight days late.</p> <p>No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance are distinguishable from the instant noncompliance and the entity promptly self-identified and mitigated the instant noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) created a new ██████████ server management group specific to the PACS servers in order to minimize the chance that they will be mismanaged in the future; 2) counseled the IT subject matter expert on the importance of adherence to documented procedures, the importance of communicating widespread changes to all impacted areas, and the importance of attention to detail and accuracy in work related to NERC CIP applicable systems; 3) counseled the CIP Team Member on the importance of adhering to documented procedures and of using incident records to track investigation and resolution of potential issues; and 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019507	CIP-010-2	R1	[REDACTED]	[REDACTED]	1/5/2018	2/12/2018	Self-Report	Completed
			4) updated the procedure for tracking the baseline to ensure that any configuration exceptions which are not accepted into the baseline are clearly documented in an incident record whose target completion date is less than thirty days from the original "[REDACTED]" before accepting any exceptions. The entity also reviewed a report of such incident records weekly at the same time the [REDACTED] is reviewed. ReliabilityFirst has verified the completion of all mitigation activity.					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017853	CIP-004-6	R4; P4.2	████████████████████	████████	10/1/2016	6/19/2017	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On June 29, 2017, ██████ submitted a Self-Report to SERC stating that, ██████ it was in noncompliance with CIP-004-6 R4, Part 4.3. The entity had one instance where it did not implement one or more documented access management program(s) that includes, for electronic access, verifying at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary. SERC later determined that this noncompliance was better addressed under CIP-004-6 R4; P4.2 because the entity did not verify at least once every calendar quarter that the individual with active electronic access had a corresponding authorization record.</p> <p>On June 16, 2017, while conducting an annual review of electronic access records, a CIP Senior Manager discovered an employee, a network administrator, provisioned with read-only electronic access to an energy management system (EMS) software application. However, the employee was not supposed to have this access. The miscue arose when the entity previously provisioned the employee with read-only access to the application to complete necessary job duties prior to commissioning of the system. Once those job duties were no longer necessary, which was prior to the October 1, 2016 effective date of CIP-004-6 R4, Part 4.2, the entity should have revoked the read-only access but did not. On June 19, 2017, the entity recognized the oversight and revoked the read-only access.</p> <p>The specific circumstances involved in discovery were that access authorization records were prepared for the transition to CIP version 5 prior to the effective date of CIP-004-6 R4, Part 4.2 on October 1, 2016. On June 16, 2017, the CIP Senior Manager compared actual access to authorization records and determined that there was one instance in which the entity provisioned access but such access was not included in the authorization records.</p> <p>The scope of affected Facilities included a primary control center, backup control center and two data centers. Affected Cyber Assets included 1 medium impact Bulk Electric System (BES) Cyber System and 14 BES Cyber Assets.</p> <p>The entity determined the extent-of-condition by implementing the annual access review that led to discovery. The entity discovered no additional instances.</p> <p>The root cause of this noncompliance was determined to be oversights in activities associated with implementing compliance with CIP version 5.</p> <p>This noncompliance started on October 1, 2016, when CIP-004-6 R4, Part 4.2 became mandatory and enforceable, and ended on June 19, 2017, when the entity revoked user access to the application.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. By not maintaining accurate authorization records, there was a partial degradation in situational awareness of access granted to an individual, and a potential avenue of exploitation by hackers to access BES Cyber Systems, gain control over facilities or system parameters and maliciously cause grid instability. However, in this instance the employee in question was a trusted network administrator with access to other BES Cyber Assets, and had a completed a Personnel Risk Assessment and taken the required cyber security training. The entity also protected the affected Cyber Assets within an Electronic Security Perimeter and Physical Security Perimeter, and employed Cyber Asset monitoring and alerting at all times. No harm is known to have occurred.</p> <p>SERC considered the entity's compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) had the CIP Senior Manager provide notice of the potential violation by email to the entity Supervisor of the CIP Group and request the unauthorized electronic access to be revoked until further review; 2) had the entity Supervisor of the CIP Group confirm that the requested revocation had occurred; 3) continued to use the entity CIP-004 Account Management Program that established the process for the provision of new and revised electronic and physical access. In this document, the entity has designated the ████████████████████ as an Account Authorizer(s) for Medium-Impact Applicable Systems, protected information, and admin/shared accounts for Applicable Systems. The Account Authorizer is responsible for reviewing and approving new access requests based upon the business need for access. The ████████████████████ is responsible for ensuring that staff transfers, standard terminations, and terminations for cause are completed based upon this program's processes. The ████████████████████ responsibilities also include the periodic review of staff access to Medium-Impact facilities and systems, protected information, and shared accounts to Applicable Systems; 4) implemented an access request form that requires a unique case that tracks the request and authorization using software; and 5) reviewed the entity's physical and electronic access rights at least once every 15 months as required by the entity CIP-004 Account Management Program. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020145	CIP-006-6	R2: P2.1	[REDACTED]	[REDACTED]	6/20/2018	6/20/2018	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On July 31, 2018, [REDACTED] submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R2. Specifically, [REDACTED] reported that on June 20, 2018, a security guard allowed three unescorted janitors to enter a Physical Security Perimeter (PSP) containing one network printer classified as a Protected Cyber Asset (PCA) associated with [REDACTED] High Impact BES Cyber System (HIBCS). The janitors were left unescorted in the PSP for 40 minutes until a Security Systems Operator investigated an alarm triggered by consecutive denials of the PSP door and discovered the janitors. The Security Systems Operator immediately escorted the janitors out of the PSP and reported the incident. [REDACTED] then performed the following: 1) physically inspected the PSP and the PCA, the janitors, their equipment, and all items (garbage) was removed from the PSP and found no suspicious activity or equipment tampering; 2) a Cyber Defense Analysis of the PCA and found no evidence of suspicious activity; and 3) conducted a comprehensive interview with the janitors, which resulted in no evidence of suspicious behavior or activity.</p> <p>After reviewing all relevant information, WECC determined that [REDACTED] failed to continuously escort visitors within its PSP as required by CIP-006-6 R2 Part 2.1.</p> <p>This noncompliance started on June 20, 2018, when three janitors were left unescorted in a PSP and ended on June 20, 2018, when the three janitors were removed from the PSP, for a total of forty minutes of noncompliance.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, [REDACTED] failed to continuously escort visitors within its PSP as required by CIP-006-6 R2 Part 2.1. Such failure could allow an unauthorized individual to physically access systems and intentionally, or accidentally, disrupt or make changes to equipment and systems. The PSP in scope of the violation contained one PCA associated with [REDACTED] HIBCS, however the printer did not have ports that could be exploited to gain access to the HIBCS. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as minor.</p> <p>[REDACTED] implemented good detective controls by identifying and responding to alarms in response to PSP access denials. Additionally, because of the network printer's physical limitation of not having any ports to exploit, the likelihood of causing potential harm was considerably limited. Based on this, WECC determined that there was a low likelihood of causing minor harm to the BPS. No harm is known to have occurred.</p> <p>WECC considered [REDACTED] compliance history in its designation of this remediated issue as a CE. [REDACTED] relevant prior compliance history with CIP-006-6 R2 includes NERC Violation ID [REDACTED]. Therefore, WECC determined that while [REDACTED] is relevant history, it is only one instance of previous noncompliance and should not serve as an aggravating factor.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) removed the janitors from the PSP; 2) met with the security guard and review the [REDACTED] Visitor Control Program elements, PSP signage, and instructions for visitor controls; 3) updated its site-specific post orders to include PSP escorting procedures; 4) delivered a PSP-focused training to CIP-certified security guards; 5) created a template with all steps required for escorting visitors in and out of a PSP; and 6) finalized documentations to facilitate consistency relative to PSP signage for HIBCS and MIBCS. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2016016415	CIP-007-6	R2, P2.2, 2.3	████████████████████	████████	7/1/2016	2/16/2018	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On October 26, 2016, ██████ submitted a Self-Report stating that, as a ██████ and a ██████, it was in noncompliance with CIP-007-6 R2.</p> <p>Specifically, ██████ reported that as part of the CIP version 5 implementation, it had implemented a patch management system to gather, evaluate and install applicable security patches. However, on July 27th a third-party vendor was engaged to replace the patch monitoring job functions of the prior Lead Information Technology (IT) technician that left employment with ██████ on June 30, 2016. The vendor was not able to achieve remote access into ██████ patch management system due to improperly maintained password files by the Lead technician who was no longer at ██████. The vendor then came onsite to fix the password issue which they resolved on August 16, 2016. On August 18, 2016, while pulling reports from the patch management system, the vendor determined that the main server was not functioning properly and was not connecting to seven Bulk Electric System (BES) Cyber Assets (BCAs), two Protected Cyber Assets (PCAs) and 12 Electronic Assess Control or Monitoring System (EACMS) associated with its Medium Impact BES Cyber System (MIBCS), nor was it collecting and aggregating security patches appropriately to those devices. The vendor was able to resolve this issue on September 1, 2016, at which time all security patches were evaluated for the 21 devices. Additionally, ██████ engaged its Physical Access Control System (PACS) vendor to review the PACS devices for compliance with the Standard and Requirement. The vendor discovered there had been no evaluation of security patches performed for 14 PACS devices since July 1, 2016, because the vendor's annual service agreement for patching services had never been approved by the facility manager who also left employment with ██████ on June 10, 2016. ██████ and the vendor resolved the contract issue and created a plan to address the evaluation of security patches for the PACS which was completed on February 16, 2017.</p> <p>After reviewing all relevant information WECC determined that ██████ failed to, at least once every 35 calendar days, evaluate security patches for applicability that had been released since the last evaluation from the source or sources identified in Part 2.1, as required by CIP-007-6 R2 Part 2.2. As a result, ██████ also failed to take action for applicable patches to either apply the patches, create a dated mitigation plan, or revise an existing mitigation plan as required by CIP-007-6 R2 Part 2.3. This failure affected seven BCAs, two PCAs, 12 EACMS, and 14 PACS devices; all associated with a MIBCS, for a total of 35 Cyber Assets.</p> <p>The root cause was due to management follow-up or monitoring of activities that did not identify problems. Specifically, there was no oversight of the work performed by former personnel related to system configuration for effective security patch evaluations. Additionally, the contract for patching services related to the PACS was never confirmed by management as being signed.</p> <p>WECC determined that the issues began July 1, 2016, when the Standard and Requirement became effective and ended on February 16, 2018 when ██████ completed its security patch evaluations and installation of applicable patches for all devices in scope, for a total of 231 days.</p>					
<p>Risk Assessment</p>			<p>WECC determined these issues posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Specifically, ██████ failed to, at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1, as required by CIP-007-6 R2 Part 2.2. As a result, ██████ also failed to take action for applicable patches to either apply the patches, create a dated mitigation plan, or revise an existing mitigation plan as required by CIP-007-6 R2 Part 2.3. This failure affected seven BCAs, two PCAs, 12 EACMS, and 14 PACS devices; all associated with MIBCS, for a total of 35 Cyber Assets. Such failures could potentially result in an attacker utilizing known security patch vulnerabilities to gain electronic and/or physical access to ██████ MIBCS to cause disruptions to its operating capabilities, potentially affecting ██████ of generation and the interconnection of ██████ and ██████ ties to the BES. WECC assessed the potential harm to the security and reliability of the BPS as intermediate.</p> <p>However, ██████ PACS were air-gapped from all other networks. As such, an attack on other networks would not have the ability to transfer to the PACS. Additionally, ██████ has cameras that could have been used forensically for security detection and were positioned to cover the internal secure areas including the Control Center. Based on this, WECC determined that there was a low likelihood of causing intermediate harm to the BPS.</p> <p>No harm is known to have occurred.</p> <p>██████ does not have any relevant previous violations of this or similar Standards and Requirements.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2016016415	CIP-007-6	R2, P2.2, 2.3	████████████████████	██████	7/1/2016	2/16/2018	Self-Report	Completed
Mitigation			<p>To remediate and mitigate this issue, ██████</p> <ol style="list-style-type: none"> 1.) Performed patch evaluations and installed applicable patches for the devices in scope; 2.) Deployed a new patch management tracker to include tracking the evaluation completion date, due date for compliance, and the action taken for applicable patches; 3.) Updated its patch management processes and procedures to include Section 5 which addresses patch management tracking, updates to processes, patch sources, mitigation plans, and identified personnel responsible for evaluating newly released security patches; 4.) Updated language related to monthly reviews of the new patch management tracker by the CIP Senior Manager or delegate to promote visibility and situational awareness; and 5.) Conducted patch management refresher training to applicable personnel to discuss change control request forms and other documentation necessary for security patch evaluations and implementation. <p>WECC verified ██████ completion of Mitigation Plan.</p>					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018018940	CIP-004-6	R4: P4.1.1.	[REDACTED]	[REDACTED]	12/12/2017	12/12/2017	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On January 3, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-004-6 R2. Specifically, [REDACTED] reported that on December 19, 2017 during a weekly meeting, it discovered that on December 12, 2017, a subcontractor was given escorted physical access to a Physical Security Perimeter (PSP) for the purpose of replacing the Physical Access Control System (PACS) panel associated with the PSP door which protected [REDACTED] Medium Impact Bulk Electric System (BES) Cyber System (MIBCS) with External Routable Connectivity (ERC). As part of the process of replacing the PACS panel, the subcontractor needed electronic access to the PACS server in order to set up communications between the new panel and the server. A [REDACTED] technician, with authorized electronic access to the server, logged in with his credentials so that the subcontractor could access the server and complete his work. The subcontractor was on site from 9:15 AM to 4:30 PM and accessed the PACS server for approximately two hours throughout the day. Even though the [REDACTED] technician was physically present for the entire time the subcontractor was accessing the server, there is no Requirement in the Standard that allows for the escorting of electronic access.</p> <p>After reviewing all relevant information, WECC determined that [REDACTED] failed to appropriately implement its process to authorize electronic access to its PACS associated with the MIBCS with ERC based on need, as required by CIP-004-6 R4 Part 4.1 Sub-Part 4.1.1. [REDACTED] not did fail CIP-004-6 R2 as originally Self-Reported.</p> <p>The root cause of the issue was due to less than adequate processes or procedures. Specifically, [REDACTED] Access Management Program at the time did not clearly define the expectations for third-party electronic access to its CIP applicable systems.</p> <p>This noncompliance started on December 12, 2017, when an unauthorized individual gained electronic access to [REDACTED] PACS server, and ended that same day, when the unauthorized individual's electronic access was removed.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, [REDACTED] failed to appropriately implement its process to authorize electronic access to its PACS associated with the MIBCS with ERC based on need, as required by CIP-004-6 R4 Part 4.1 Sub-Part 4.1.1. Such failure could allow a malicious actor to adjust the settings on the PACS such as turning off alarms, which would limit situational awareness, or allow unrestricted access to the MIBCS by adjusting or removing access rights. [REDACTED] owns and/or operates [REDACTED] of generating capacity with a peak load of [REDACTED] that was applicable to this issue. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as minor.</p> <p>However, [REDACTED] had weak controls in place to prevent this issue. The only compensating factor was the subcontractor being continuously escorted while in the PSP and on the server. Based on this, WECC determined that there was a moderate likelihood of causing minor harm to the BPS. No harm is known to have occurred.</p> <p>WECC considered [REDACTED] compliance history in its designation of this remediated issue as a CE. [REDACTED] prior compliance history with CIP-004-6 R4 includes NERC Violation IDs [REDACTED] and [REDACTED]. WECC determined that [REDACTED] is not relevant compliance history as it deals with keeping the list updated when changes occur, which is different from this noncompliance. Additionally, WECC determined that while [REDACTED] is relevant compliance history, it is only one instance of previous noncompliance and should not serve as an aggravating factor to escalate the disposition.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) removed the unauthorized electronic access from the subcontractor; 2) updated its program to clearly define that it will not grant unauthorized electronic access and will not allow electronic access escorting; 3) updated its process to review its CIP-004 Access Management Program with all appropriate personnel at least once every 15 calendar months; and 4) provided CIP-004 training to appropriate personnel. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018481	CIP-010-2	R2; P2.1	[REDACTED]	[REDACTED]	8/8/2016	10/25/2016	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-010-2 R2.</p> <p>Specifically, [REDACTED] reported that while conducting its 2016 internal compliance assessment it identified four instances where the baseline configuration monitoring exceeded the 35-days required by CIP-010-2 R2 Part 2.1. [REDACTED] was generally performing the required baseline configuration monitoring automatically via its SIEM, however the Cyber Assets associated with this issue did not interface well with the SIEM so the 35-day reviews were being conducted manually. The four instances were related to three Electronic Access Control or Monitoring System (EACMS) Cyber Assets that are associated with its High Impact BES Cyber Systems (HIBCSs) located at [REDACTED] data center and its primary and backup Control Centers. The first EACMS was a two-factor authentication device which provided the second form of authentication when connecting to the Virtual Private Network (VPN) for remote access into the HIBCS. The VPN configuration determined the access level permissions for the users when connecting. The VPN was configured to allow managed remote access for 146 people when connecting to the HIBCS. The second and third EACMS are an Intrusion Detection Sensor (IDS) management server and its IDS sensor that monitors network traffic and security events from [REDACTED] HIBCS and its Medium Impact BES Cyber System (MIBCS) located at the [REDACTED] station.</p> <p>After reviewing all relevant information, WECC determined that [REDACTED] failed to have a documented process or procedure to manually perform the activities required by CIP-010-2 R2 Part 2.1. In addition, [REDACTED] also failed, in four separate instances, to monitor at least once every 35 calendar days for changes to the baseline configuration, as required by CIP-010-2 R2 Part 2.1.</p> <p>The root cause of these issues was a lack of documented process or procedure. Specifically, there were no formalized process documents to perform Part 2.1 manually. The [REDACTED] analyst used internal knowledge and a ticketing system.</p> <p>WECC determined that the start date for the earliest issue began on August 8, 2016, the 36th day of [REDACTED] not having monitored the baseline configuration and ended on October 25, 2016, when [REDACTED] performed monitoring of the baseline configuration. The longest duration was 14 days.</p>					
Risk Assessment			<p>WECC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In these instances, [REDACTED] on four separate occasions, failed to have a documented process or procedure to manually perform the activities required by CIP-010-2 R2 Part 2.1. In addition, [REDACTED] also failed, in four separate instances, to monitor at least once every 35 calendar days for changes to the baseline configuration, as required by CIP-010-2 R2 Part 2.1. Such failure could cause the authentication device to not function as intended which could affect remote user connectivity into the HIBCS and MIBCS. Without the required second form of authentication, remote users would be unable to login which could prevent system administrators from monitoring fault conditions or viewing real-time events. An unauthorized change to the IDS server or the IDS sensor could potentially cause security events alerting to fail or to go unnoticed by systems personnel. [REDACTED] had a system peak load of [REDACTED] and one generation plan with [REDACTED] total capacity that was applicable to this issue. Remote access into the PCC and BCC would be affected. If there was an event at the same time within the PCC, remote users would not be able to login and troubleshoot any issues. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as intermediate.</p> <p>However, [REDACTED] In addition, access to the EACMS Cyber Assets in scope was limited to authorized employees. There was also a comprehensive procedure for making any changes to the EACMS. Lastly, the duration of each instance of noncompliance was very short. For these reasons, WECC determined that there was a low likelihood of causing intermediate harm to the BPS. No harm is known to have occurred.</p> <p>WECC determined that [REDACTED] has no relevant compliance history for this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) performed baseline configuration manual monitoring for all Cyber Assets in scope; 2) created a detailed workflow procedure for manual baseline configuration monitoring and added the process to its procedure documentation; 3) updated the workflow management system to include scheduled task alerts for manual baseline monitoring prior to the task deadline; and 4) conducted training on the updated procedures and tasks with all personnel responsible for baseline configuration monitoring. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018481	CIP-010-2	R2; P2.1	[REDACTED]	[REDACTED]	8/8/2016	10/25/2016	Self-Report	Completed
			WECC has verified the completion of all mitigation activity.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018585	CIP-007-6	R4, P4.2, P4.2.2	[REDACTED]	[REDACTED]	7/1/2016	10/12/2017	Compliance Audit	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], WECC auditors determined that [REDACTED] as a [REDACTED] and [REDACTED], had a potential noncompliance with CIP-007-6 R4.</p> <p>Specifically, [REDACTED] reported it had not generated alerts for security events that included an alert for detecting failure of Part 4.1 event logging for one Electronic Access Control or Monitoring System (EACMS) associated with its Medium Impact Bulk Electric System (BES) Cyber System (MIBCS) at a substation. It was determined that during [REDACTED] transition to CIP Version 5, several upgrades were implemented to its Security Incident and Event Management (SIEM) server. Subsequently, the transfer of the firewall logging rules had inadvertently dropped a line which prevented logging communication for devices queried through the firewall. As these logs were not included in the SIEM logging, the alerts failed, including failure of logging alerts. Additionally, [REDACTED] did not generate alerts for security events to include the detected failure of event logging for five EACMS used to allow remote access to the MIBCS, and one Physical Access Control System (PACS) associated with its High Impact BES Cyber System (HIBCS) due to a misconfiguration of the logging aggregator that passed logs to the SIEM. As a result of the SIEM not receiving the logs, alerts could not be generated to include detected failures for logging.</p> <p>After reviewing all relevant information, WECC determined that [REDACTED] failed to generate alerts for security events that it determined necessitated an alert, that included, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): detected failure of Part 4.1 event logging for six EACMS and one PACS, as required by CIP-007-6 R4 Part 4.2 Sub-Part 4.2.2.</p> <p>The root cause of this issue was due to a lack of validation or verification of the accuracy of a change. Specifically, [REDACTED] did not perform testing or validate configuration changes on all assets due to the volume of assets being implemented during the CIP Version 5 transition.</p> <p>WECC determined that this issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to [REDACTED] and ended on October 12, 2017, when alerts were generated, for a total of 469 days.</p>					
Risk Assessment			<p>WECC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, [REDACTED] failed to generate alerts for security events that the [REDACTED] determined necessitate an alert, that included, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): detected failure of Part 4.1 event logging, for the devices in scope, as required by CIP-007-6 R4 Part 4.2 Sub-Part 4.2.2. Such failure could potentially result in security events occurring without the knowledge of these logins or login attempts that include both successful and unsuccessful login events on the EACMS associated with the MIBCS at its substation that had [REDACTED]. Failing to generate alerts for security events on one of the EACMS jump-hosts, PACS devices or database servers associated with its MIBCS or HIBCS, at the data center or primary Control Center, could result in a malicious actor gaining electronic and/or physical access and [REDACTED] personnel would be unaware of the security events. Failure of these assets could result in authorized remote users not being able to login to substations or data center assets. If a malicious attacker successfully logged into substation assets they could potentially cause a failure of transmission operations. An unknown attack on data center assets could potentially cause a loss of critical data or affect data center operations at the primary Control Center. [REDACTED] oversees a peak load of [REDACTED] and [REDACTED] of generation, and approximately [REDACTED] miles of transmission which included [REDACTED] miles of [REDACTED] miles of [REDACTED] and [REDACTED] miles of [REDACTED] all of which could have been affected by this issue. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as intermediate.</p> <p>However, [REDACTED] personnel retained visibility through logs and alert capability from adjacent security systems. This increased the likelihood that suspicious activity would be detected from multiple sources and provided the organization context to ensure attacks were detected regardless of origination. Based on this, WECC determined that there was a low likelihood of causing intermediate harm to the BPS.</p> <p>No harm is known to have occurred.</p> <p>[REDACTED] does not have any relevant previous violations of this or similar Standards and Requirements.</p>					
Mitigation			<p>To remediate and mitigate this issue, [REDACTED]</p> <ol style="list-style-type: none"> 1.) added the firewall rule to allow devices to send logs to the SIEM and resume alerting; 2.) corrected the data source group configuration for the five EACMS devices; 3.) rebooted the PACS server to resolve the system error and resume alerting; 4.) implemented a procedure to verify all data sources were accounted for during similar changes; and 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018585	CIP-007-6	R4, P4.2, P4.2.2	[REDACTED]	[REDACTED]	7/1/2016	10/12/2017	Compliance Audit	Completed
			5.) increased the local log size to allow more logs to be stored to prevent an alerting gap from occurring if a system error occurs on a logging aggregator. WECC verified [REDACTED] completion of Mitigation Plan.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018586	CIP-014-2	R4	██████████ (████)	██████████	1/27/2016	4/5/2016	Compliance Audit	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from ██████████, WECC auditors determined that ██████ as a ██████████, and ██████████, had a potential noncompliance with CIP-014-2 R4 and R5.</p> <p>Specifically, ██████ provided evidence that it completed R4 and R5 of CIP-014-2 on April 5, 2016, which was 189 days after it completed R2.</p> <p>After reviewing all the relevant information, WECC determined that ██████ failed to: 1) conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of its respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in CIP-014-2 R1 and verified according to R2 as required by CIP-014-2 R4, within the required NERC implementation timeline; and 2) failed to develop and implement a documented physical security plan that covers its respective Transmission station(s), Transmission substation(s), and primary control center(s) within the required NERC implementation timeline as required by CIP-014-2 R5. Although the CIP-014 Standard does not explicitly state a timeframe in which R4 should be completed, FERC's final rule on Order No. 802 approved NERC's Physical Security Reliability Standard implementation timeline.</p> <p>The root cause of the noncompliance was ██████ relied on a table of implementation dates provided in various outreach presentations. The table listed the requirements and the activities, the implementation timeline and a column entitled "Not Later Than". ██████ understood the "Not Later Than" date as the initial implementation date.</p> <p>WECC determined that these issues began on January 27, 2016, which was 120 days after ██████ completed CIP-014-2 R2, and ended on April 5, 2016, when ██████ completed R4 and R5, for a total of 69 days of noncompliance.</p>					
Risk Assessment			<p>WECC determined that this noncompliance posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In this instance, ██████ failed to conduct an evaluation of the potential threats and vulnerabilities of a physical attack, as required by CIP-014-2 R4, for each of its respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in CIP-014-2 R1 and verified according to R2 within the required NERC implementation timeline, and failed to develop and implement a documented physical security plan that covers its respective Transmission station(s), Transmission substation(s), and primary control center(s) within the required implementation timeline, as required by CIP-014-2 R5. Such failure could lead to further delays in addressing the threats and vulnerabilities identified in R4. This delay could allow a potential attacker more time to impact the facilities, which if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. ██████ transmission system consists of approximately ██████ miles of transmission which includes ██████ miles of ██████ lines, ██████ miles of ██████ lines, and ██████ miles of ██████ lines. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as intermediate.</p> <p>However, ██████ completed R4 and R5 69 days beyond the required implementation plan. Both the threat and vulnerability assessment required by R4 and the physical security plan required by R5 were found to be compliant in every other respect by the WECC auditors. Based on this, WECC determined that there was a low likelihood of causing intermediate harm to the BPS. No harm is known to have occurred.</p> <p>WECC determined that ██████ has no relevant compliance history for this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, ██████</p> <ol style="list-style-type: none"> 1) held a kick-off meeting for the next R1 Transmission Risk Assessment, at which time attendees discussed timelines; the audit finding; and recommendations received from the audit; 2) scheduled on-going status meetings to track progress and timelines and to facilitate communication between business areas; 3) added CIP-014-2 compliance activities and deadlines into its ServiceNow tracking system; and 4) adopted a date calculator to track the calculation of dates to ensure future dates are not missed. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018587	CIP-014-2	R5	██████████	██████████	1/27/2016	4/5/2016	Compliance Audit	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from ██████████, WECC auditors determined that ██████ as a ██████████, and ██████████, had a potential noncompliance with CIP-014-2 R4 and R5.</p> <p>Specifically, ██████ provided evidence that it completed R4 and R5 of CIP-014-2 on April 5, 2016, which was 189 days after it completed R2.</p> <p>After reviewing all the relevant information, WECC determined that ██████ failed to: 1) conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of its respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in CIP-014-2 R1 and verified according to R2 as required by CIP-014-2 R4, within the required NERC implementation timeline; and 2) failed to develop and implement a documented physical security plan that covers its respective Transmission station(s), Transmission substation(s), and primary control center(s) within the required NERC implementation timeline as required by CIP-014-2 R5. Although the CIP-014 Standard does not explicitly state a timeframe in which R4 should be completed, FERC's final rule on Order No. 802 approved NERC's Physical Security Reliability Standard implementation timeline.</p> <p>The root cause of the noncompliance was ██████ relied on a table of implementation dates provided in various outreach presentations. The table listed the requirements and the activities, the implementation timeline and a column entitled "Not Later Than". ██████ understood the "Not Later Than" date as the initial implementation date.</p> <p>WECC determined that these issues began on January 27, 2016, which was 120 days after ██████ completed CIP-014-2 R2, and ended on April 5, 2016, when ██████ completed R4 and R5, for a total of 69 days of noncompliance.</p>					
Risk Assessment			<p>WECC determined that this noncompliance posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In this instance, ██████ failed to conduct an evaluation of the potential threats and vulnerabilities of a physical attack, as required by CIP-014-2 R4, for each of its respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in CIP-014-2 R1 and verified according to R2 within the required NERC implementation timeline, and failed to develop and implement a documented physical security plan that covers its respective Transmission station(s), Transmission substation(s), and primary control center(s) within the required implementation timeline, as required by CIP-014-2 R5. Such failure could lead to further delays in addressing the threats and vulnerabilities identified in R4. This delay could allow a potential attacker more time to impact the facilities which if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. ██████ transmission system consists of approximately ██████ miles of transmission which includes ██████ miles of ██████ lines, ██████ miles of ██████ lines, and ██████ miles of ██████ lines. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as intermediate.</p> <p>However, ██████ completed R4 and R5 69 days beyond the required implementation plan. Both the threat and vulnerability assessment required by R4 and the physical security plan required by R5 were found to be compliant in every other respect by the WECC auditors. Based on this, WECC determined that there was a low likelihood of causing intermediate harm to the BPS. No harm is known to have occurred.</p> <p>WECC determined that ██████ has no relevant compliance history for this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, ██████</p> <ol style="list-style-type: none"> 1) held a kick-off meeting for the next R1 Transmission Risk Assessment, at which time attendees discussed timelines; the audit finding; and recommendations received from the audit; 2) scheduled on-going status meetings to track progress and timelines and to facilitate communication between business areas; 3) added CIP-014-2 compliance activities and deadlines into its ServiceNow tracking system; and 4) adopted a date calculator to track the calculation of dates to ensure future dates are not missed. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017879	CIP-007-6	R4; P4.1; P4.3	[REDACTED]	[REDACTED]	7/1/2016	9/26/2016	Self-Report	Completed
<p>Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On July 7, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-007-6 R4.</p> <p>Specifically, [REDACTED] reported that during a change control review conducted in September 2016, it identified an instance in which it failed to capture and retain 90 calendar days of security event logs for one Electronic Access Control or Monitoring System (EACMS) which did not have a Security Incident and Event Manager (SIEM) log collector installed, and two network switches which were improperly configured and did not have a firewall rule in place to enable log collection to the SIEM; all associated with a Medium Impact BES Cyber System (MIBCS). Additionally, [REDACTED] reported that during a Cyber Vulnerability Assessment (CVA) it identified one EACMS associated with a High Impact Bulk Electric System (BES) Cyber System (HIBCS) that was not capturing and retaining security event logs due to configuration errors on the SIEM device which caused a gap in logging. The SIEM was collecting and storing all logs sent to the device from other devices, but was not logging failed login attempts to itself. The SIEM was inadvertently disabled during a recent upgrade to the device.</p> <p>After reviewing all relevant information, WECC determined [REDACTED] failed to capture and retain security event logs, per BES Cyber Asset capability, for all cyber security events as required by CIP-007-6 R4 Part 4.1 Sub-Parts 4.1.1 and 4.1.2 and R4.3, for four Cyber Assets.</p> <p>The root cause of the noncompliance was insufficient manpower to support goals and objectives. Specifically, during the transition from CIP Version 3 to CIP Version 5, asset configuration changes were not tested or peer reviewed before implementation.</p> <p>WECC determined that events began when [REDACTED] failed to log and retain security event logs on July 1, 2016 and ended on September 26, 2016 when [REDACTED] started logging and retaining security event logs as required by CIP-007-6 R4, Part 4.1, Sub-Parts 4.1.1, 4.1.2, and Part 4.3, for a total of 88 days.</p>					
<p>Risk Assessment</p>			<p>WECC determined that this noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, [REDACTED] failed to capture and retain security event logs, per BES Cyber Asset capability, for all cyber security events as required by CIP-007-6 R4 Part 4.1 Sub-Parts 4.1.1 and 4.1.2 and R4.3, for four Cyber Assets. Such failure could allow a malicious actor to login to the devices without [REDACTED] knowledge. A failure to retain ninety days of logs would prevent [REDACTED] from being able to review the security details for after-the-fact investigations. This could potentially cause a loss of remote access and SCADA data for series capacitors on one of the [REDACTED] lines which include [REDACTED]. A potential loss of other devices at a [REDACTED] substation could potentially cause a loss of remote access to meters, however data is still sent to Electronic Monitoring System (EMS) via serial cable at this location. [REDACTED] owns and operates [REDACTED] of [REDACTED] generation, and [REDACTED] of generation in their [REDACTED] footprint. [REDACTED] transmission system consists of approximately [REDACTED] miles of transmission which includes [REDACTED] miles of [REDACTED] lines, [REDACTED] miles of [REDACTED] lines, and [REDACTED] miles of [REDACTED] lines. WECC assessed the potential harm to the security and reliability of the BPS as intermediate.</p> <p>However, [REDACTED] Cyber Assets were physically secured as well as isolated from the internet and internal networks by utilizing network segmentation to include firewalls that deny access by default. In the event a system would have gone down or resource usage was abnormal, [REDACTED] Systems or Network and Telephone Services teams would have received notification and troubleshooting would have taken place to identify the root cause and any attack would have been identified as part of their troubleshooting. The primary physical monitoring of the BES Cyber System is performed in real-time at the Physical Security Command Center which is manned twenty-four hours a day. Based on this, WECC determined that there was a low likelihood of causing intermediate harm to the BPS. No harm is known to have occurred.</p> <p>WECC determined that [REDACTED] compliance history should not serve as a basis for applying a penalty. There was a different cause for the prior instances of noncompliance which was distinct and separate than the cause of this issue.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) restarted the SIEM logging service to enable log collection and storage of logs; 2) installed the SIEM collector on applicable device; 3) added firewall rules to allow logs to send to the log collectors; 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

Western Electricity Coordinating Council (WECC)

Compliance Exception

CIP

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017879	CIP-007-6	R4; P4.1; P4.3	[REDACTED]	[REDACTED]	7/1/2016	9/26/2016	Self-Report	Completed
			4) added a peer review step in its change control process to be performed before the change ticket can be closed; 5) implemented new change controls templates to ensure CIP security controls are completed and applied; 6) conducted CIP device owner training to include CIP-007-6 R4 logging and monitoring and the change control overview process; and 7) implemented device owner training tracking to ensure all device owners have received the enhanced training.					